《붉은별》 봉사기용체계 3.0
사용지도서
(1)

차 례

머 리 말

위대한 령도자 **김정일**동지께서는 다음과 같이 지적하시였습니다.

《프로그람을 개발하는데서 기본은 우리 식의 프로그람을 개발하는것입니다. 우리는 우리 식의 프로그람을 개발하는 방향으로 나가야 합니다.》

(《**김정일**선집》 제15권, 196페지)

정보기술이 급속히 발전하고있는 현시기 날로 늘어나는 방대한 량의 쏘프트웨어 및 자료들을 보호하고 그 안전성을 담보하자면 우리 식의 조작체계를 받아들이는것이 매우 중요하게 제기됩니다.

《붉은별》 봉사기용체계 3.0은 원천이 공개된 최신판본의 Linux조작체계에 기초하여 새롭게 개발한 우리 식 조작체계로서 우리 식의 보안기능과 여러가지 망봉사기능을 제공하고있는 강력한 조작체계입니다.

《붉은별》 봉사기용체계 3.0은 핵심부준위에서의 보안강화와 보안관리자와 체계관리자의 구분, 체계의 완전성을 검사하는 기능, 빠른 설치를 보장하였으며 가상화기능을 리용한 봉사효률을 제고하였습니다. 또한 이전 판본들과의 사용자대면부에서의 차이는 도형방식사용자대면부(GUI)가 아니라 문자방식사용자대면부(CUI)를 지원한것입니다. 문자방식사용자대면부는 조작성이 도형방식사용자대면부에 비해보면 떨어지지만 봉사기의 자원효률성을 높이고 안정성을 높이는데서 우월합니다. 조작성을 높이기 위하여 원격으로 충분히 봉사기를 관리할수 있는 통합봉사기관리도구《빛발》3.0을 갱신하여 추가하였습니다.

《붉은별》 봉사기용체계 3.0사용지도서는 크게 2개부로 구성하였습니다. 1부에서는 국부관리방식을 위주로 관리방법을 서술하였으며 2부에서는 통합봉사기관리도구《빛발》3.0에 대하여 서술하였습니다.

이 사용지도서는 《붉은별》 봉사기용체계 3.0을 처음으로 리용하는 체계관리자 및 사용자들이 지령입력에 의한 기초적인 체계조작과 관리방법을 쉽게 배울수 있도록 서술하였습니다.

이 사용지도서는 총 8개의 장으로 구성되였습니다.

제1장과 제 2장에서는 《붉은별》 봉사기용체계 3.0을 처음 리용하는 사용자들을 위하여 체계의 설치와 체계의 기동과 끝내기, 가입방법 등에 대하여 설명하고있습니다.

제3장에서는 체계관리자 및 보안관리자들이 조작탁에서 여러가지 봉사기들을 설정하고 관리하는 빙법에 대하여 설명하고있습니다.

제4장에서는 체계관리와 관련한 체계설정 및 관리방법에 대하여 설명합니다.

제5장에서는 개척자화일체계의 설치 및 검사, 이름관리방법들에 대하여 설명하고있습니다.

제6장에서는《붉은별》 봉사기용체계 3.0의 보안을 실현하고있는 접근조종방식과 방화벽관리도구의 설치 및 관리방법에 대하여 설명하고있습니다.

제7장에서는 iSCSi와 dmraid, mdadm, LVM2들을 설치하고 이러한 기억장치들을 관리하는 방법들에 대하여 설명하고있습니다.

제8장에서는《붉은별》 봉사기용체계 3.0의 가상화환경설치와 가상조작체계관리방법에 대하여 설명하고있습니다.

우리는 하루빨리 《붉은별》 봉사기용체계 3.0의 구성원리와 사용방법을 습득함으로써 우리 식의 쏘프트웨어를 보다 높은 수준에서 개발하는데서 나서는 과학기술적문제들을 원만히 해결하는데 이바지하여야 합니다.

제1장. 《붉은별》봉사기용체계 3.0의 설치

이 장에서는《붉은별》 봉사기용체계 3.0의 설치방법에 대하여 설명합니다.

제1절. 설치환경

《붉은별》 봉사기용체계 3.0을 설치하려면 다음의 하드웨어조건을 만족하여야 합니다.

- 체계설치에 필요한 하드웨어조건은 다음과 같습니다.

·각종 봉사기

·PC

표 1. 장치환경

환경 / 장치	최소환경 (32Bit/64Bit 체계)	표준환경 (32Bit/64Bit 체계)
CPU	Pentium IV 3GHz/ 64Bit x86 확장기능	Core T Duo 2GHz/ 64Bit x86 확장기능
주기억	1GB	2G 이상
HD	5GB	10GB
망기판	1 개	1 개

제2절. 설치방법

매개 설치단계마다 〈확인〉단추를 눌러 설치를 진행합니다.

1. 작업의 시작

《붉은별》 봉사기용체계 3.0설치프로그람의 기동방법에 대하여 서술합니다.

-CD로부터의 작업시작

우선 콤퓨터가 CD-ROM으로 기동하도록 하기 위하여 BIOS(Basic Input/Output System)의 기동항목(Boot option)을 변경합니다.

콤퓨터에 전원을 넣고 콤퓨터가 기동하면 설치프로그람이 기동합니다.

-《붉은별》 봉사기용체계 3.0의 이전판본의 GRUB(기동적재프로그람)를 리용한 작업시작

GRUB의 편집환경에서 배포판의 vmlinuz와 initrd.img를 지정합니다.

실례:

```
grub> root (hd0,5)
        grub>kernel /vmlinuz
        grub>initrd /initrd.img
        grub>boot
```

-grub4dos 프로그람을 리용한 작업시작

MS-DOS기동디스크로 MS-DOS를 기동시키고 grub4dos프로그람을 실행시킵니다. 프로그람의 Command Line항목을 선택하면 GRUB가 실행됩니다.

다음의 조작은 GRUB를 리용한 조작실례와 같습니다.

2. 인증코드 입력

《붉은별》 봉사기용체계 3.0은 정당한 사용자(해당한 절차를 걸쳐 구입한 사용자)만이 사용할수 있습니다.

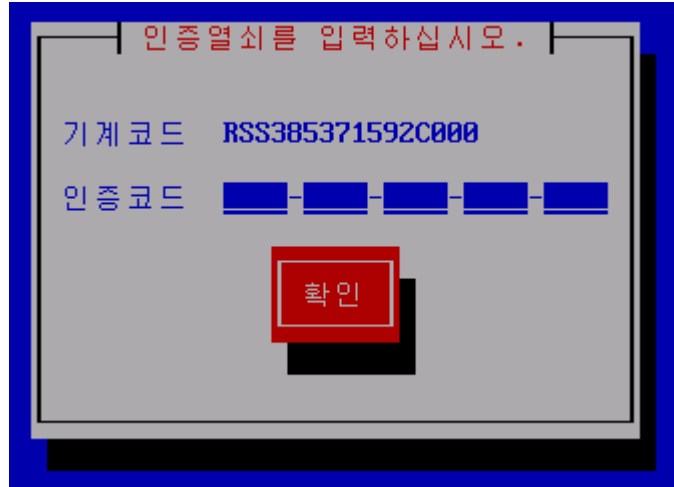



그림 1. 인증열쇠입력

체계의 비법사용을 막기 위하여 사용자인증을 진행합니다.

사용하려는 기대의 식별번호에 기초한 인증코드를 구입지로부터 받은 사용자는 인증코드입력칸에 열쇠를 입력하고 〈확인〉 단추를 누릅니다.

인증코드가 없는 사용자는 체계를 설치할수 없습니다.

3. 망설정

체계의 망대면을 설정합니다.

사용자는 설치되는 체계의 IP주소를 설정합니다.

체계는 IPv4와 IPv6을 지원하며 주소할당은 사용자의 선택에 따라 자동 혹은 수동으로 설정할수 있습니다.

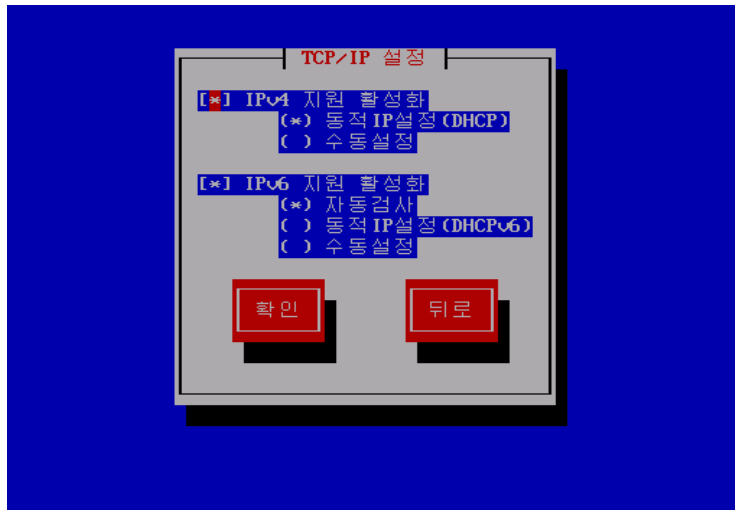



그림 2. 망설정

4. 설치방법

《붉은별》 봉사기용체계 3.0설치는 설치매체의 형태에 따라 다양한 설치방법을 제공합니다.

그림 3. 설치방법

- [국부 CD/DVD] – 설치영상이 CD에 있는 경우

  사용자가 CD로 설치를 시작한 경우에 선택합니다.

- [하드구동기] – 설치영상이 하드구동기에 있는 경우

  하드구동기에 설치영상이 있는 경우에는 이 항목을 선택하고 경로를 입력하여야 합니다.

- [NFS등록부] 와 [URL] – 설치영상이 봉사기에 있는 경우

  이 설치방법을 망에서의 설치라고도 합니다.

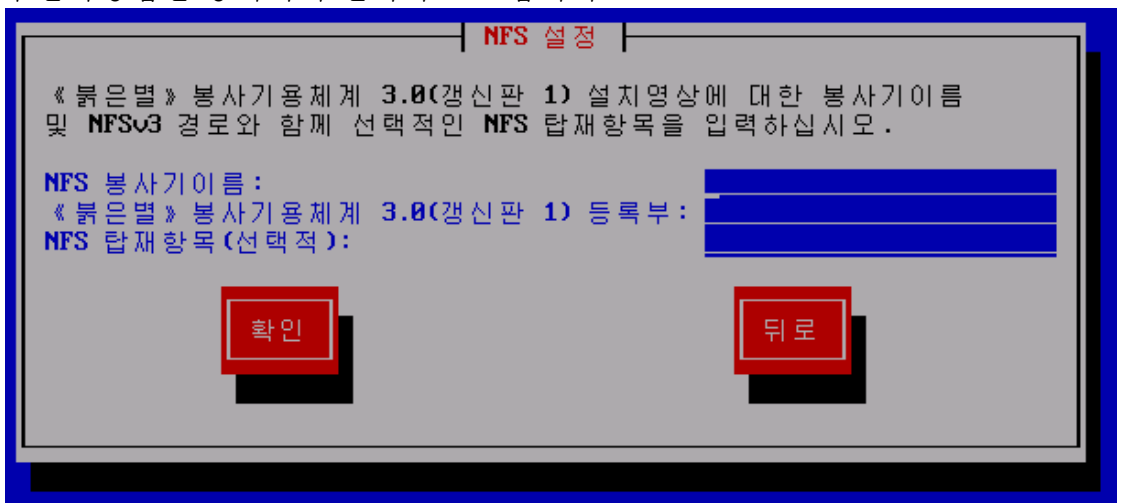



그림 4. NFS 설정

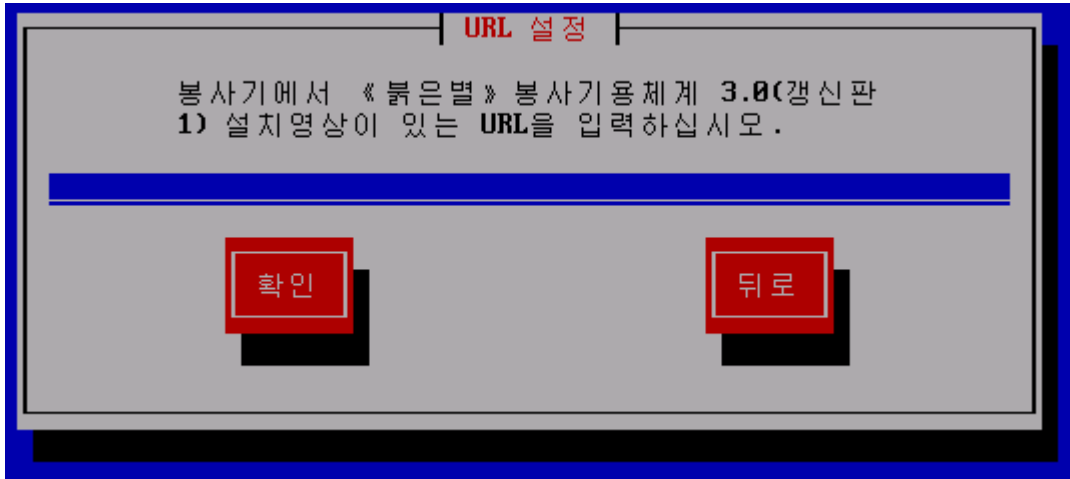



그림 5. URL 설정

설치쏘프트웨어는 설정된 경로에서 설치영상을 내리적재하여 설치를 진행합니다.

5. 관리자암호설정

체계관리자는 체계전반관리를 진행하는 사용자입니다. 체계관리자암호는 수자와 영문자, 특수문자의 조합으로 6문자이상으로 만들어야 합니다.

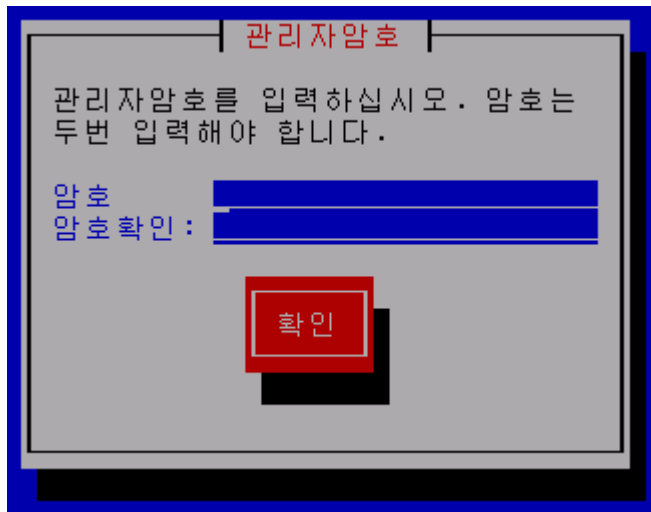



그림 6. 관리자암호설정

6. 구획설정

[전체구동기사용]

이 항목을 설정하면 모든 구동기를 체계구획으로 설정합니다.

[기존체계교체]

이미 설치되여있는 구획을 초기화하고 여기에 체계를 설치합니다.

[여유공간사용]

디스크공간을 검사하고 여유공간에 체계를 설치합니다.

[전용구획설정]

사용자의 설정에 따라 구획을 분리하고 체계를 설치합니다.

사용자는 구획관리대면부를 통하여 구획을 관리할수 있습니다.

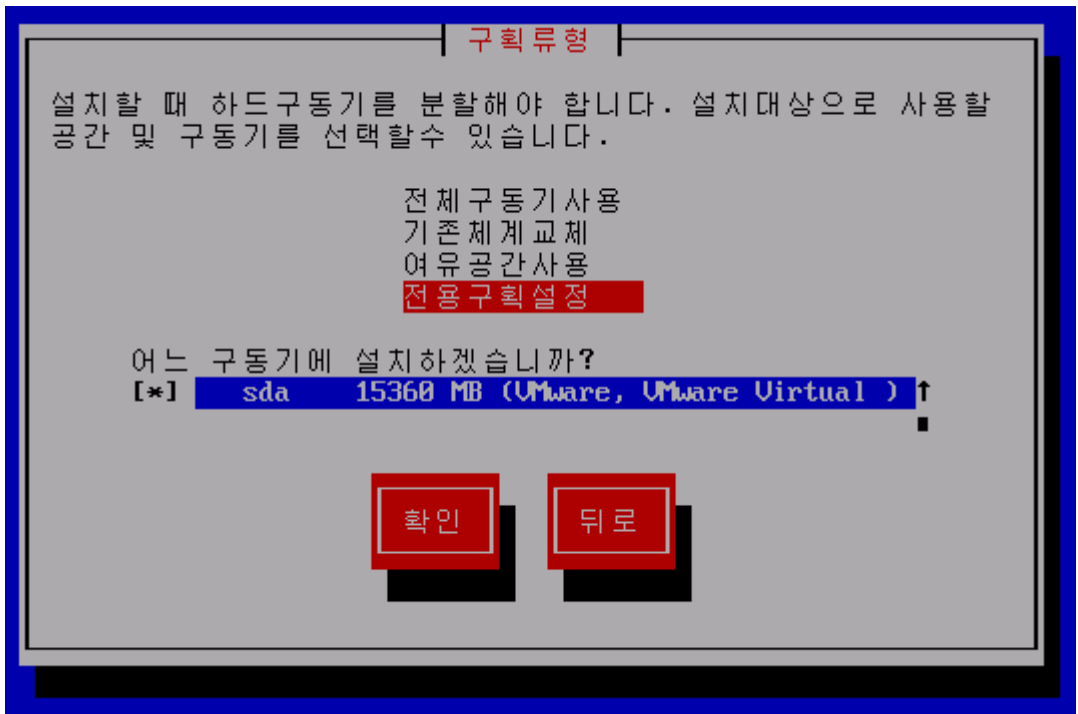



그림 7. 구획설정

구획관리대면부에서는 구획의 생성, 삭제, 편집 등 조작을 진행합니다.

일반적으로 하드디스크의 사용효률을 높이기 위하여 하드디스크를 여러개의 구획으로 갈라놓고 사용합니다.

구획에는 기본구획과 확장구획, 론리구획이 있는데 하나의 하드디스크에는 최대로 4개의 기본구획을 만들수 있습니다.

기본구획가운데서 하나를 확장구획으로 만들수 있는데 확장구획은 기본구획과는 다르게 여러개의 론리구획으로 나눌수 있습니다.

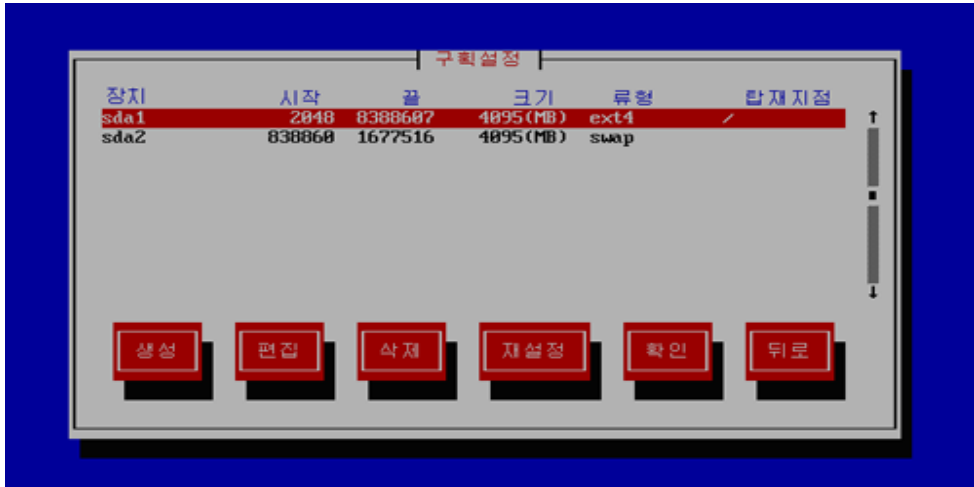



그림 8. 전용구획설정

기본구획은 1~4까지 수자가 붙으며(실례로 IDE하드디스크의 첫번째 기본구획인 경우 《/dev/hda1》로 됩니다.) 론리구획은 반드시 5부터 번호가 붙습니다.

《붉은별》 봉사기용체계 3.0에서는 Windows에서와 같이 구동기개념이 없으며 개별적인 구획들을 개개의 등록부에 련결(탑재)하여 리용합니다.

《붉은별》 봉사기용체계 3.0에서는 여러개의 구획들을 생성하고 아래의 표와 같은 탑재지점에 탑재하여 리용할수 있습니다.

표 2. 탑재지점목록

탑재지점 혹은 탑재등록부	의 미
/	《붉은별》 봉사기용체계 3.0 에서 뿌리등록부입니다.
/boot	체계기동에 필요한 화일들을 보관하고있는 등록부입니다.
/home	일반사용자의 정보보관용등록부인데 이 등록부이름은 home 이 아니라 사용자식별이름으로 됩니다.

/usr	《붉은별》 봉사기용체계 3.0을 처음 설치할 때 대부분의 응용쏘프트웨어들이 보관되는 등록부입니다.
/usr/local	일반적으로 추가로 설치하는 응용쏘프트웨어들이 보관되여있는 등록부입니다.
/var	각종 기록정보화일과 우편화일 보관되는 등록부입니다.
/tmp	림시보관용 등록부입니다.
/opt	Oracle과 같은 응용쏘프트웨어들이 설치되는 등록부입니다.

《붉은별》 봉사기용체계 3.0을 설치할 때 뿌리구획(/)과 교환구획만 만들어주어도 되지만 우에서와 같이 구획을 여러개로 만들어 리용하면 여러가지 좋은 점이 있습니다.

우선 비정상적인 체계완료로 하여 다음번 체계기동시 구획검사를 하는데 뿌리구획하나만 있는 경우 검사시간이 길어져서 체계기동이 떠질수 있습니다.

다음으로 구획에 오유가 발생하는 경우 다른 구획의 자료를 보호할수 있습니다. 뿌리구획이 하나만 있고 그 구획이 파괴되는 경우 모든 자료가 분실될수 있는데 구획을 여러개 만들어 놓고 탑재하여 리용하면 어느 한 구획이 파괴되여도 다른구획의 자료는 보호할수 있습니다.

《붉은별》 봉사기용체계 3.0을 설치하기 위한 구획설정창문은 하드디스크의 설정상태를 보여주는 도형과 설정단추모임, 구획상태를 보여주는 창문으로 구성되여있습니다.

■ 설정단추모임

설정단추모임은 생성, 편집, 삭제, 재설정단추들로 구성되여있습니다.

표 3. 설정단추모임

단 추	설 명
생 성	구획을 새로 만들 때 리용합니다.
편 집	이미 존재하는 구획을 수정하는데 리용합니다.
삭 제	구획을 삭제할 때 사용합니다.
재설정	구획표를 재설정합니다.

■ 구획상태창문

하드디스크의 이름과 구획의 상세한 정보를 보여주는 창문입니다.

표 4. 구획설정항목

창 문 요 소	설 명
장 치	구획이 속한 하드디스크이름을 표시합니다.
탑재지점/RAID	탑재할 지점을 표시합니다.
류 형	구획의 화일체계류형을 말합니다. (실례로 개척자,FAT32, ext2,ext3,ext4)
초기화	구획이 만들어지면 초기화가 된다는것을 표시합니다.
용 량	구획의 크기를 표시합니다.
시작, 끝	구획의 시작과 마지막 분구를 표시합니다.

참고 : 분구는 하드디스크나 흘로피디스크와 같은 디스크모양의 매체에서 기록단위를 말합니다. 나무의 년륜과 같이 나누어 놓은 자리길을 방사선모양으로 나누어 놓은것입니다. 매체마다 자리길당 분구의 수는 서로 다릅니다.

■ 구획추가

구획을 추가하기 위하여서는 하드디스크의 빈구역을 선택하고 〈생성〉단추를 누릅니다. 이때 아래의 그림과 같은 구획추가창문이 표시됩니다.

그림 9. 구획추가화면

구획추가화면의 입력요소들은 다음과 같습니다.

표 5. 구획추가화면의 입력요소

창문요소	설 명
탑재지점	탑재지점을 나타냅니다. 건반으로 직접 입력할수도 있고 일반적으로 많이 사용하거나 반드시 필요한 부분은 선택할수 있습니다.
화일체계류형	추가되는 구획의 화일체계형태를 선택할수 있습니다. 일반적으로 교환구획을 제외하고는 개척자 2을 선택하면 됩니다.
용 량	추가하려는 구획의 크기를 지적합니다.
추가용량 선택항목	일반적으로 고정용량항목을 선택하고 마지막에 최대 가능한 용량으로 채우기항목를 선택합니다. 고정용량항목을 선택하여야 마지막에 남은 크기를 지정할 때 최대 가능한 용량으로 채우기항목을 선택하더라도 용량크기에 변화가 없습니다.
기본구획으로 강제설정	추가하는 구획을 강제적으로 기본구획으로 만들려고 할 때 선택합니다.

▸ /구획만들기

/구획만들기는 반드시 생성하여야 할 화일체계의 뿌리등록부입니다.

/구획만들기를 만들기 위하여서는 탑재지점에 /를 선택합니다.

그리고 구획의 크기를 설정하고 화일체계류형을 개척자2로 선택한 다음 〈확인〉 단추를 누릅니다.

참고 : 기본구획만들기에서 주의할 점
1) 기본구획은 한개 디스크에서 3 개 미만이여야 합니다.
2) /구획은 용량은 5GB 이상이여야 합니다.
우의 두가지 경우에는 하드디스크에 빈공간이 있다고 하여도 구획이 창조되지 않습니다.

▸ 교환구획 만들기

교환구획은 주기억기용량이 작은 경우 하드디스크의 일정한 부분을 가상기억기로 쓰기 위하여 사용되는 공간입니다.

교환구획을 만들기 위하여서는 화일체계류형을 [교환구획]로 선택하고 구획의 크기를 주기억기용량이 2GB보다 작으면 그의 2배되게 2GB보다 크다면 2GB로 지정한 다음 〈확인〉 단추를 누릅니다.

참고 : 교환구획만들기에서 주의할 점
1) 기본구획창조를 진행한 다음 교환구획을 창조하는것이 좋습니다.
2) 교환구획의 위치는 디스크의 첫부분(primary partition) 혹은 확장 구획의 첫부분에 놓이지 말아야 합니다.

■ 구획편집

구획을 편집하기 위하여서는 하드디스크의 편집가능한 구획을 선택하고 편집단추를 누르면 됩니다.

이때 구획편집창문이 표시됩니다.

구획편집창문에서는 구획의 탑재지점의 변경과 구획의 초기화설정만을 진행할수 있습니다.

■ 구획삭제

구획을 삭제하기 위하여서는 삭제하려는 구획을 선택하고 삭제단추를 누릅니다. 이때 삭제확인창문이 표시되는데 이 창문에서 삭제단추를 누르면 됩니다.

7. 기동적재기 설정

기동적재기는 체계기동관리쏘프트웨어로서 조작체계를 기동(boot)시키기 위한 중요한 쏘프트웨어입니다.

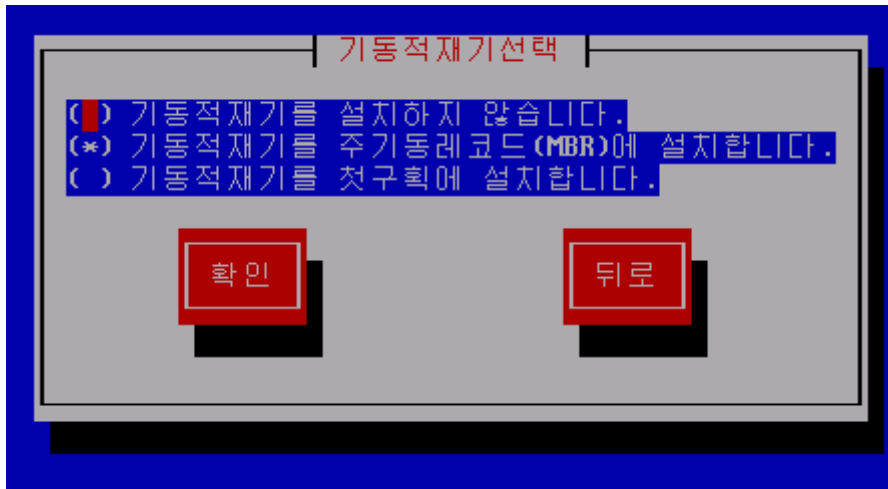



그림 10. 기동적재기설정

> **참고 :** 기동(boot)은 콤퓨터의 전원을 투입한 때로부터 사용자가 조작할 수 있게 될 때까지 콤퓨터가 자동적으로 진행하는 일련의 동작을 의미합니다. 전원을 투입하면 BIOS(기본입출력체계)의 PL(쏘프트웨어초기적재기)이 하드웨어의 초기화를 진행한 후 기동디스크의 MBR(master boot record)를 검색하고 그 정보에 따라 기동가능한 구획의 기동코드를 읽어 들이고 조작체계를 기억기 에 불러 들여 조작체계에 대하여 사용자의 조작이 가능한 상태로 되게 합니다.

《붉은별》 봉사기용체계 3.0을 설치할 때 표준적으로 리용되는 기동적재기는 GRUB(GRand Unified Bootloader)입니다.

GRUB는 여러가지 조작체계들을 기동시킬수 있는 강력한 쏘프트웨어입니다.

기동적재기창문의 항목은 다음과 같습니다.

— 기동적재기가 설치될 위치

기동적재기는 표준적으로 《붉은별》 봉사기용체계 3.0을 설치하는 하드디스크의 첫번째 분구(MBR - Master Boot Record)에 설치됩니다. 그러나 다른 조작

체계의 기동적재기(실례로 Boot Magic와 같은)가 첫번째 분구에 설치되여있으면 《붉은별》 봉사기용체계 3.0이 설치되는 구획은 시작분구에 설치할수 있습니다.

《붉은별》 봉사기용체계 3.0이 설치되는 구획의 첫번째 분구에 기동적재기를 설치하려면 《/dev/hd* (SATA혹은 SCSI하드디스크인 경우 /dev/sd*)구획의 첫번째 분구》항목을 선택하면 됩니다. 이때는 MBR에 설치 된 다른 조작체계의 기동적재기가 우선권을 가지고 먼저 동작하게 됩니다.

8. 패키지선택

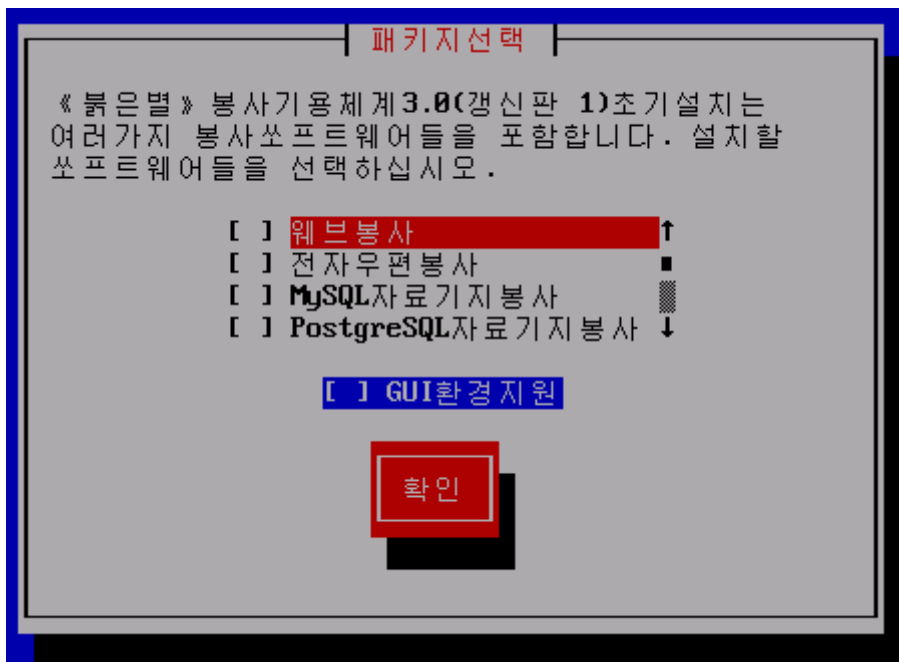
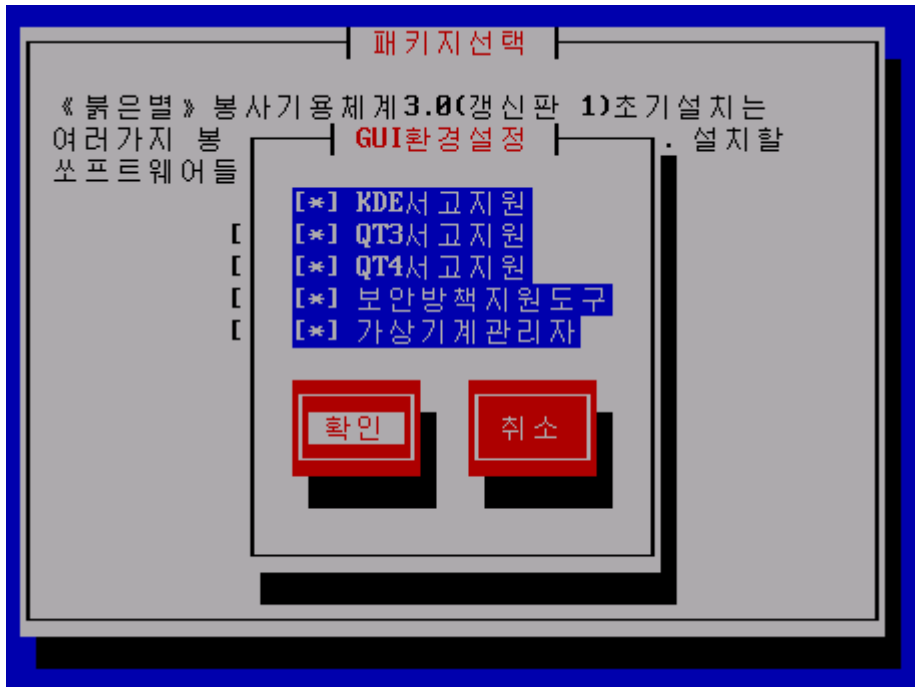



그림 11. 패키지선택

기동적재기선택이 완료되면 봉사기체계에서 리용되는 봉사쏘프트웨어 및 관리도구들을 선택적으로 설치할수 있습니다.

사용자는 봉사기의 사명에 따라 해당한 봉사쏘프트웨어들을 선택할수 있습니다.

GUI환경지원을 선택하면 KDE, QT3, QT4서고들과 보안방책지원도구, 가상기계관리자를 선택할수 있습니다.

보안방책지원도구와 가상기계관리자는 패키지선택창에서 보안체계지원, 가상화지원이 선택되여야 GUI환경설정창에서 설정할수 있습니다.

9. 패키지설치

선택된 쏘프트웨어에 대한 의존성검사를 진행하고 선택된 구획에 체계패키지를 설치합니다.

그림 12. 패키지설치

10. 설치완료

그림 13. 체계설치완료창문

체계설치가 끝나면 완료창문이 표시됩니다.

체계설치완료창문에서 재기동단추를 눌러 콤퓨터를 재기동합니다.

제2장. 체계기동과 가입,가입탈퇴

제1절. 체계의 기동과 끝내기

1. 체계의 기동

① 콤퓨터에 전원을 넣습니다.

② 기동화면이 나옵니다.

그림 14. 체계기동화면

③ 아무런 건반조작을 하지 않아도 《붉은별》 봉사기용체계 3.0이 기동합니다.

참고 : 체계기동과정에 대한 정보를 보려면 F2건을 누르면 됩니다.

주의 : 체계기동시 체계구획에 적어도 300M정도의 여유공간이 있어야 합니다. 여유공간이 없으면 체계가 파괴될 위험성이 있습니다.

2. 체계의 끝내기

① 조작탁에서 init 0 , 또는 poweroff명령을 실행합니다.

② 콤퓨터의 전원이 차단됩니다.

제2절. 기동적재기

1. 개요

여기서는 사용자들이 기동적재기를 사용하는 방법을 설명합니다.

Linux조작체계는 일반적으로 다국어처리환경을 원만하게 지원하고있습니다. 그러나 기동적재기(grub)는 다국어처리지원이 되여있지 않습니다.

《붉은별》 봉사기용체계 3.0에서는 기동적재기의 국문화를 실현함으로써 조선어환경을 실현합니다.

즉 우리 식 조작체계에서 기동적재기의 국문화를 실현하여 사용자들이 국문화된 환경에서 기동적재기를 사용할수 있습니다.

기동적재기의 설치는 《붉은별》 봉사기용체계 3.0을 설치하는 경우 자동설치됩니다.

2. 사용방법

시작안내문에서 명시적으로 설정된 안내문에서 Enter건으로 기동하면《붉은별》 봉사기용체계 3.0이 기동합니다.

제3절. 체계의 가입과 탈퇴

체계가입과 탈퇴는 체계에 등록된 사용자를 알려주어 개인화일을 보호 하고 자기의 설정을 보존하도록 하는 기능입니다.

1. 체계가입

사용자가 자기의 이름과 암호를 가지고 체계를 기동시키는 기능입니다.

사용자는 이름과 암호를 체계에 등록함으로써 자기의 개인화일들을 다른 사용자들의 접근으로부터 보호합니다.

《붉은별》 봉사기용체계 3.0에서 관리자이름은 기정으로 root로 되여있습니다

- 체계가입화면에서 관리자이름을 입력하고 Enter건을 누릅니다.
- 관리자암호를 입력하고 Enter건을 누릅니다.
- 그러면 관리자의 권한으로 체계에 가입합니다. 관리자이름이나 암호가 틀리는 경우 가입이 실패하며 가입을 다시 진행해야 합니다.
- 체계가입이 정확히 진행되면 조작탁화면이 현시됩니다.

만일《붉은별》 봉사기용체계 3.0에서 위임접근조종을 시행하고있다면 《제6장 보안관리》를 참고하십시오.

2. 체계탈퇴

- 조작탁에서 logout명령을 실행합니다.
- 체계가입화면이 현시됩니다.

제3장. 체계설정

제1절. 날자와 시간

체계날자와 시간은 관리자만이 설정할수 있습니다.
체계날자와 시간정보를 확인, 설정하기 위하여서는 date 지령을 리용합니다.
다음과 같은 지령행으로 체계날자 및 시간을 확인할수 있습니다.

```
#date
```

체계날자 및 시간을 설정하려면 "date MMDDhhmm[[CC]YY][.ss]"와 같은 형식을 리용하거나 date 지령의 –s 선택항목을 리용하여야 합니다.
형식문자렬 "MMDDhhmm[[CC]YY][.ss]"의 의미는 다음과 같습니다.

MM	월
DD	일
hh	시
mm	분
CC	년도의 첫 두 수자(선택적입니다.)
YY	년도의 마지막 두 수자(선택적입니다.)
ss	초(선택적입니다.)

체계는 기동할 때 CMOS 로부터 하드웨어시간정보를 얻어 설정합니다.
CMOS 에 들어 있는 하드웨어시간을 확인하기 위하여서는 clock 지령을 리용하여야 합니다.
다음의 지령행으로 체계의 하드웨어시간을 확인할수 있습니다.

```
#clock -r
```

체계시간을 하드웨어시간으로 설정하려면 다음의 지령행을 리용하면 됩니다.

```
#clock -w
```

하드웨어시간을 체계시간으로 설정하려면 다음의 지령행을 리용하면 됩니다.

```
#clock –s
```

제2절. 망설정

망설정은 체계설정편의프로그람 setup 을 리용하여 진행할수 있습니다.
setup 을 리용하는 경우 창문환경에서 망설정을 진행하므로 아주 편리합니다.

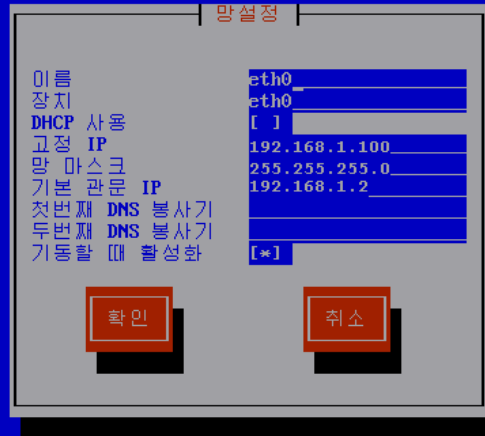



그림 15. setup 지령에서 망설정

또한 체계가 제공하는 지령들인 ip 나 ifconfig, netstat, route 를 리용하여 망설정을 진행할수 있습니다.

ifconfig 지령을 리용하여 망대면부 eth0 을 가동하려면 다음의 지령행을 리용하면 됩니다.

```
ifconfig eth0 up
```

망대면부 eth0 을 중지하려면

```
ifconfig eth0 down
```

을 리용하면 됩니다.

실례로 망대면부 eth0 의 IP 주소를 192.168.1.100 으로 설정하는 경우 다음과 같은 지령행을 리용할수 있습니다.

```
ifconfig eth0 192.168.1.100 netmask 255.255.255.0
```

또한 설정화일들을 변경하고 그것을 체계에 반영하는 방법으로 망설정을 진행할수 있습니다.

망설정관련화일들에는 /etc/sysconfig/network, /etc/sysconfig/network-scripts/ifcfg-eth0 등이 있습니다.

망설정화일 /etc/sysconfig/network 화일에는 통신지원여부를 설정하는 항목 NETWORKING, 주콤퓨터이름설정항목 HOSTNAME, 관문설정항목 GATEWAY 등이 있습니다.

화일 /etc/sysconfig/network 의 내용실례는 다음과 같습니다.

```
NETWORKING=yes
HOSTNAME=server.edu.kp
GATEWAY=192.168.1.2
```

화일 /etc/sysconfig/network-scripts/ifcfg-eth0 은 망대면부 eth0 과 관련된 설정을 진행하는 화일입니다.

이 화일의 내용실례는 다음과 같습니다.

```
DEVICE=eth0
IPADDR=192.168.1.100
NETMASK=255.255.255.0
BROADCAST=192.168.1.255
NETWORK=192.168.1.0
ONBOOT=yes
```

여기서 선택항목 DEVICE 는 망장치대면부의 이름, IPADDR 는 해당 대면부의 IP 주소, NETMASK 는 망마스크값, BROADCAST 는 방송망 IP 주소, NETWORK 는 망의 주소, ONBOOT 는 체계기동시 망대면부활성여부를 설정합니다.

설정화일들을 변경한 후 망봉사를 재시작하는 방법으로 그 내용을 체계에 반영할수 있습니다.

망봉사를 재시작하는 지령행은 다음과 같습니다.

```
#service  network restart
```

제3절. 봉사설정

봉사설정은 체계설정편의프로그람 setup 을 리용하여 진행할수 있습니다.

그림 16.　 setup 지령에서 봉사설정

또한 지령 service, chkconfig 를 리용하여 진행할수 있습니다.

service 지령을 리용하여 봉사의 시작, 중지, 재시작을 진행할수 있습니다.

service 지령의 일반적인 지령형식은 다음과 같습니다.

service {봉사이름} [start | restart | stop]

실례로 service 지령을 리용하여 망봉사 network 를 시작하려면 다음의 지령행을 리용할수 있습니다.

#service network start

network 봉사를 중지하려면

#service network stop

지령행을 리용하면 됩니다.

chkconfig 지령을 리용하면 매 실행방식마다 봉사시작여부를 설정할수 있습니다.

실례로 chkconfig 지령을 리용하여 망봉사가 모든 실행방식에서 시작하도록 설정하려면

chkconfig –level 2345 network on

지령행을 리용하면 됩니다.

제4절. 암호변경

통과암호는 passwd 지령을 리용하여 설정할수 있습니다.

실례로 사용자 guest 의 통과암호를 변경하려면

passwd guest

라는 지령행을 실행한 다음 새로운 암호를 입력한 다음 그것을 확인하기 위해 다시 암호를 입력한 후 ENTER 건을 누르면 됩니다.

관리자암호를 설정, 변경하기 위하여서는 관리자계산자리로 체계에 가입하여야 합니다.
관리자는 모든 사용자들의 암호를 설정할수 있습니다.
사용자이름을 지적하지 않고 passwd 지령을 실행하는 경우 관리자의 암호를 변경하게 됩니다.

제5절. CPU 전력관리

CPU 전력관리는 봉사기의 CPU 에서 소모되는 전력을 절약하기 위한 쏘프트웨어입니다.
쏘프트웨어는 체계가 기동하면서 자동적으로 실행되며 환경설정 및 조종은 통합봉사기관리도구 《빛발》3.0 에서 진행합니다.

1.《CPU 전력관리》설치와 삭제

《CPU 전력관리》는《붉은별》 봉사기용체계 3.0 을 완전히 설치하면 설치됩니다.

① 하드웨어동작환경

Intel 및 AMD 계렬의 DVS(동적박자주파수조종)기능을 지원하고있는 CPU 를 사용하여야 합니다.
CPU 박자주파수 800MHz 이상, 주기억 128MB 이상
하드용량 1MB, 매일 기동시에 기록화일을 저장하므로 2MB/일 이상의 여유공간

② 《CPU 전력관리》설치와 삭제

《CPU 전력관리》의 설치는《붉은별》 봉사기용체계 3.0 의 쏘프트웨어설치방식에 따릅니다.

－ 설치시 주의사항

《CPU 전력관리》는《붉은별》 봉사기용체계 3.0 을 완전히 설치하면 설치됩니다.

－ 설치

설치하려면 cps-1.1.0.i686.rpm 화일이 있어야 합니다.
조작탁에서 다음과 같이 입력합니다.

```
rpm -ivh --force cps-1.1.0.i686.rpm
```

－ 삭제

《CPU 전력관리》를 삭제하려면 조작탁에서 다음과 같이 입력합니다.

```
rpm -e cps
```

그러면 《CPU 전력관리》는 체계에서 삭제됩니다.

2.《CPU 전력관리》리용

1) 《CPU 전력관리》의 시작

쏘프트웨어를 설치하면 조작체계가 기동할 때 자동적으로 CPU 전력관리봉사가 시작됩니다. 쏘프트웨어를 조종하기 위하여서는 통합봉사기관리도구《빛발》3.0 을 기동하고 《체계》->《CPU 전력관리 설정》을 선택합니다.

환경설정 및 조종과 관련한 도움말은 《도움말》->《CPU 전력관리 설정》에서 볼수 있습니다.

2) 전력조종파라메터 설정

전력조종파라메터는 다음과 같습니다.

최대동작시간

봉사기는 어떤 시간동안 최대의 부하를 받고 다른 구간에서는 부하가 상대적으로 작습니다. 실례로 어떤 웨브봉사기는 오전 첫시간과 점심시간에 최대의 부하를 받고 나머지시간에는 거의 부하를 받지 않습니다. 이렇게 부하가 최대로 되는 시간에는 봉사기의 성능을 최대로 높일 필요가 있습니다. 최대동작시간은 이러한 최대부하시간을 지정하는 파라메터입니다.

최대동작시간은 시간대들의 모임으로 이루어집니다. 시간대란 시작시간과 끝시간으로 구성된 시간쌍으로서 특정한 시간구간을 나타내는 값입니다. 최대동작시간에는 여러개의 시간대가 포함될수 있습니다. 일반적으로 콤퓨터(봉사기)의 부하가 최대로 되는 시간을 설정합니다.

최대주파수턱값

CPU 의 박자주파수를 최대동작속도로 올려야 할 사용률 턱값입니다.

·최소주파수턱값

CPU 의 박자주파수를 최소동작속도로 낮추어야 할 사용률 턱값입니다.

·주파수올림턱값

CPU 의 박자주파수를 한단계 높은 속도로 올려야 할 사용률 턱값입니다.

주파수내림턱값

CPU 의 박자주파수를 한 단계 낮은 속도로 낮추어야 할 사용률 턱값입니다.

주파수조종간격

CPU 의 박자주파수를 조종하는 시간간격입니다.

·기록간격

CPU의 사용률 및 박자주파수를 기록하는 시간간격입니다. 현재 주파수조종을 진행한 후 기록을 진행하므로 이 설정항목의 내용은 의미가 없습니다.

이 파라메터들에 의하여 CPU박자주파수는 다음과 같은 순서로 조종됩니다.

걸음 1. 현재 시간이 최대동작시간에 속하면 CPU주파수를 최대로 설정하고 걸음 1로 갑니다.

걸음 2. CPU의 사용률정보(퍼센트값)을 얻습니다.

걸음 3..사용률이 최대동작속도 사용률보다 크면 CPU주파수를 최대로 설정하고 걸음 1로 갑니다.

걸음 4..사용률이 동작속도증가 사용률보다 크면 CPU주파수를 한단계 높은 주파수로 설정하고 걸음 1로 갑니다.

걸음 5. 사용률이 동작속도감소 사용률보다 작으면 CPU주파수를 한단계 낮은 주파수로 설정하고 걸음 1로 갑니다.

− 최대동작시간 설정

최대동작시간은 봉사기의 부하가 최대로 된다고 예측되는 시간입니다. 봉사기의 부하가 최대로 되는 시간에 CPU의 박자주파수를 낮추면 봉사성능을 떨구게 되므로 이 시간에는 CPU박자주파수를 최대로 설정합니다.

최대동작시간은 **시작시간~끝시간**의 형식으로 이루어진 시간구간들의 모임으로 설정합니다. 매 시간은 24시간형식으로서 **시간:분**으로 구성합니다. 매 시간구간은 한행에 놓여야 하며 서로 사귈수 있습니다.

실례: 08:30~09:20

이와 같은 문법을 지키지 않은 행들은 무시합니다. 최대동작시간을 변경하고 보관을 누른 후 변경적용을 하여야 변경내용이 적용됩니다.

− 일반설정

일반설정에서는 최대주파수턱값, 최소주파수턱값, 주파수올림턱값, 주파수내림턱값, 주파수조종간격, 기록간격을 설정합니다.

− 설정보관

보관단추를 눌러 설정내용을 보관합니다.

설정된 파라메터 및 설정내용이 유효하게 하려면 설정을 보관하고 CPU박자주파수조종봉사를 재시작하여야 합니다.

3) CPU전력관리봉사의 조종

전력관리조종단추는 세가지, 즉 시작, 중지, 재시작단추가 있습니다. 시작단추는 CPU 박자주파수조종봉사를 시작하는 단추이며 중지단추는 중지시키는 단추입니다. 변경적용단추는 봉사를 다시 시작하는 단추로서 이 단추를 누르는 경우의 동작은 먼저 중지단추를 누르고 다음 시작단추를 누른 동작과 같습니다.

이 단추들은 봉사의 진행상황에 따라 보임상태가 자동적으로 바뀝니다.

4) CPU 박자주파수보기

CPU 박자주파수의 변화상태를 보려면 《CPU 박자주파수보기》를 선택합니다. 첫번째 CPU(CPU0)의 박자주파수를 본문과 그라프로 현시합니다. CPU 전력관리쏘프트웨어가 설정내용대로 정확히 동작하는가를 확인하는데 리용합니다.

제6절. 체계완전성관리

1. 개요

체계완전성검사도구는 악의있는 사용자가 고의로 혹은 체계관리자가 실수로 체계화일들에 대한 완전성변경을 진행하였을 때 그것을 검출하여 기록하는 쏘프트웨어입니다.

체계완전성검사도구는 수동적으로, 또는 체계가 기동할 때와 체계가동중에 실시간적으로 체계화일들의 완전성상태를 검사합니다.

완전성검사에서 기준으로 되는 표본자료기지는 사전에 준비되여있으며 필요에 따라 갱신할수도 있습니다.

체계완전성검사도구는 완전성이 변경된 화일들의 목록과 그 변경상황을 지정된 기록화일에 기록합니다.

체계완전성검사도구는《붉은별》 봉사기용체계 3.0 에 포함되여 설치됩니다.

2. 사용방법

1) 기록화일의 열람

완전성변경이 검출된 체계화일들에 대한 정보는 기록화일 /var/log/intcheck.log 에 기록되여있습니다.

쉘지령 cat, more, less 등을 리용하여 기록화일의 내용을 열람할수 있습니다.

화일안에는 완전성변경사건들에 대한 정보가 행단위로 기록되여있습니다.

한 행안에는 완전성변경이 검출된 날자 및 시간, 검출한 쏘프트웨어이름, 화일이름, 검출회수 등 여러 마당들이 구성되여있습니다.

2) 검사지표설정관리

체계완전성검사도구는 등록된 체계화일들의 여러 지표들에 대한 완전성감시여부를 확정하는 편의프로그람를 제공합니다.

체계완전성검사도구에 등록된 주목화일 /bin/sh 의 수정시간지표에 대한 검사를 진행하지 않도록 하려면 다음과 같은 지령행을 리용하면 됩니다.

```
icmgr –u –s mtime /bin/sh
```

/bin/sh 의 모든 지표에 대한 검사를 진행하도록 하려면 다음과 같은 지령행을 리용하면 됩니다.

```
icmgr –s all /bin/sh
```

3) 실시간검사기능관리

실시간검사기능은 체계화일의 완전성변경을 실시간으로 감시 및 검출하여 체계사용자들에게 통보하고 화일에 기록하는 기능입니다.

체계완전성검사도구가 제공하는 실시간검사기능을 관리할수 있는 방법은 다음과 같습니다.

① 실시간검사기능의 림시중지

아래의 지령을 리용하여 현재 가동중인 실시간검사기능을 림시로 중지할수 있습니다.

```
#service   intcheckd stop
```

② 실시간검사기능의 재개

아래의 지령을 리용하여 림시중지상태인 실시간검사기능을 재개할수 있습니다.

```
#service   intcheckd start
```

③ 실시간검사기능의 설정

아래의 지령을 리용하여 체계기동시 실시간검사기능을 실행하도록 설정할수 있습니다.

```
chkconfig –level 2345 intcheckd on
```

④ 실시간검사기능의 설정해제

아래의 지령을 리용하여 체계가 기동시 실시간검사기능을 실행하지 않도록 설정할수 있습니다.

```
chkconfig –level 2345 intcheckd off
```

4) 체계기동시 자동검사기능관리

체계기동시 자동검사기능은 말그대로 체계가 기동할 때마다 전반적인 체계화일들의 완전성을 검사하는 기능입니다.

체계완전성검사도구가 제공하는 체계기동시 자동검사기능을 관리할수 있는 방법은 다음과 같습니다.

① 체계기동시 자동검사기능의 설정

아래의 지령을 리용하여 체계가 기동시 자동검사기능을 실행하도록 설정할수 있습니다.

```
intcheck-boot on
```

② 체계기동시 자동검사기능의 설정해제

아래의 지령을 리용하여 체계가 기동시 자동검사기능을 실행하지 않도록 설정할수 있습니다.

```
intcheck-boot off
```

5) 표본자료기지의 갱신

표본자료기지는 체계화일들의 완전성지표를 보관하고있으며 실지 화일들의 완전성지표계산 및 비교에서 기준으로 되는 자료기지입니다.

다음과 같은 지령행을 리용하여 체계완전성검사도구의 표본자료기지의 전체 내용을 현재 체계와 동일하게 갱신할수 있습니다.

```
icmgr --init
```

개별적인 체계화일 실례로 /bin/cat의 모든 완전성지표만을 갱신하려면 다음과 같은 지령행을 리용할수 있습니다.

```
icmgr –p –c all /bin/cat
```

6) 도움말 열람

체계완전성검사도구에서 도움말은 man페지형식으로 제공됩니다.

따라서 도움말열람은 다음의 지령행과 같이 man지령을 리용하여 진행할수 있습니다.

```
man intcheck
```

제4장. 보안관리

제1절. 접근조종

1.개요

《붉은별》 봉사기용체계 3.0 에서 체계보안방책은 핵심부준위에서 위임접근조종을 실현하기 위한 규칙들을 서술하고있습니다.

접근조종체계는 체계보안방책에 기초하여 체계의 기밀성과 완전성을 실현하여 체계의 보안을 강화하고있습니다.

체계보안방책은 selinux-policy-3.7.19-54 패키지에 의해 실현되였습니다.

이 사용지도서는《붉은별》 봉사기용체계 3.0 을 리용하는 관리자(체계관리자와 보안관리자)들을 대상으로 하여 작성하였습니다.

관리자들은 이 사용지도서를 통하여 위임접근조종이 시행되고있는 체계에서의 체계관리방법과 보안방책설정방법들을 습득할수 있습니다.

※ 용어 및 략어해설

보안방책(security policy)
체계의 관리 및 보호방법과 정보의 접근조종방법을 규정하고있는 규칙의 집합입니다. 여러가지 형태의 보안방책들중에서 체계전반에 대한 위임접근조종을 실현하는 보안방책을 론의합니다.

역할기초의 접근조종(RBAC: Role Based Access Control)
어떤 자원에 대한 접근권한을 사용자에게 직접 할당하지 않고 주어진 체계환경에서 정의된 역할들에 할당하는 방법으로 체계자원에 대한 접근을 조종합니다.

자유접근조종(DAC: Discretionary Access Control)
자원의 소유자가 접근조종을 책임지고 접근허가를 부여하는 접근조종입니다.

위임접근조종(MAC: Mandatory Access Control)
체계가 접근조종을 책임지고 접근허가를 부여하는 접근조종입니다.

다중준위보안(MLS: Multi Level Security)
주동체와 객체에 할당한 보안준위에 기초하여 접근조종을 진행합니다.
다중분류보안(MCS: Multi Category Security)
주동체와 객체에 할당한 보안분류에 기초하여 접근조종을 진행합니다.

보안표제(security label)
체계에서 어떤 객체에 대해 필요한 보안속성을 나타내는 정보입니다.

형(type)
위임접근조종의 실현을 위해 체계내의 매 객체에 할당되고 그것에 의해 접근허가 또는 거부가 결정되는 표제입니다.

령역(domain)
위임접근조종을 실현하기 위하여 체계에서 프로쎄스에 할당되는 형입니다.

역할 (role)
사용자가 권한을 가지고있는 령역들의 집합입니다.

보안문맥(security context)
보안속성을 나타내는 가변길이 문자렬입니다.

보안식별자(SID: Security IDentifier)
체계가 보안문맥에 할당한 정수입니다. 체계만이 보안식별자를 해석할수 있습니다.

이행(transition)
보안문맥이 요구하는 연산의 목적을 결정합니다.
이행에는 두가지 중요한 형의 이행이 있는데 하나는 지정된 형의 프로쎄스를 실행했을 때 사용되는 프로쎄스령역의 이행(령역이행)이고 다른하나는 특정한 등록부에 있는 화일을 생성했을 때 사용되는 화일형의 이행(형이행)입니다.

1) 사용목적
《붉은별》 봉사기용체계 3.0에서는 다른 조작체계에서와는 달리 root관리자의 권한을 제한하여 체계의 완전성을 높이는것을 보안목표로 설정하였습니다.
조작체계에서 시행하고있는 위임접근조종방책은 역할기초의 접근조종(RBAC)모형과 형시행(TE)모형에 기초하여 작성되여있습니다.
조작체계에서는 root관리자라고 하여도 체계의 정상가동에 영향을 주는 동작을 취할수 없도록 보안방책에 의하여 체계자원에 대한 완전성보호를 실현하였습니다.
또한 위임접근조종을 시행하고있는 방책과 그 설정화일들에 대한 관리를 체계관리자권한이 아니라 보안관리자권한으로 진행할수 있도록 실현하였습니다.

2) 화일목록

보안방책을 포함하고있는 기본패키지는 다음과 같습니다.

selinux-policy-3.7.19-54.RSS3.noarch.rpm
selinux-policy-rss-3.7.19-54.RSS3.noarch.rpm
selinux-policy-targeted-3.7.19-54.RSS3.noarch.rpm

의존성패키지들은 다음과 같습니다.

checkpolicy-2.0.22-1.RSS3.i686.rpm
libselinux-2.0.94-2.RSS3.i686.rpm
libselinux-python-2.0.94-2.RSS3.i686.rpm
libselinux-utils-2.0.94-2.RSS3.i686.rpm
libsemanage-2.0.43-4.RSS3.i686.rpm
libsemenage-python-2.0.43-4.RSS3.i686.rpm
libsepol-2.0.41-3.RSS3.i686.rpm
policycoreutils-2.0.83-19.8.RSS3.i686.rpm
policycoreutils-newrole-2.0.83-19.8.RSS3.i686.rpm
policycoreutils-python-2.0.83-19.8.RSS3.i686.rpm

3) 쏘프트웨어 구성관계

《붉은별》 봉사기용체계 3.0 에서 위임접근조종을 실현하고있는 체계보안방책은 핵심부준위에서 실현되여있습니다.

체계보안방책은 체계의 기동과 체계가입, 체계봉사대몬의 관리, 응용쏘프트웨어의 실행을 비롯하여 모든 프로쎄스들을 제한하는 규칙들과 체계자원에 대한 사용자들의 접근을 제한하는 규칙들로 구성되여있습니다.

이 규칙은 policy.24 라는 2 진방책화일과 *.pp 로 된 2 진모듈방책화일들에 서술되여있습니다.

방책화일들과 그와 련관된 방책구성화일들은 전체적으로 16MByte 정도의 크기를 가집니다.

4) 우발사고시 조작과 여러 조작상태들과 방식들

본 제품은 체계관리자를 비롯하여 봉사기를 리용하는 사용자들에 대한 접근을 조종함으로써 조작체계의 완전성을 실현하고있습니다.

따라서 체계관리자들의 조작상 실수나 비법적인 사용자들의 조작으로 인하여 조작체계가 비정상적으로 가동하는 경우는 거의나 일어나지 않을수 있습니다.

이와 같은 접근조종을 시행하고있는 보안방책에 대한 관리는 보안관리자에 의해서 진행되며 보안관리자의 조작상 실수를 비롯하여 여러가지 요인들에 의하여 보안방책이 파괴되는 경우가 존재할수 있습니다.

이때 관리자는 전문가에게 문의하여 처리하여야 합니다.

참고 : 체계관리자들은 체계봉사대몬이 기동하지 않거나 체계구성을 변경할수 없는 경우에 부닥칠수 있습니다. 이것은 체계보안방책이

체계관리자의 요구를 체계완전성의 견지에서 거부하기때문입니다. 체계운영상 이상의 요구를 반드시 실현해야 하는 경우에는 보안방책관리자와의 협의하에 보안취약점을 확인하고 제기되는것이 없다고 결정한 다음 보안방책에 반영해주어야 합니다. 보안방책관리자는 핵심부 감시 및 기록체계(audit)에 의하여 제공되는 기록화일들에 기초하여 보안방책을 편집할수 있습니다. 새로운 봉사대몬을 추가하거나 새로운 체계관리쏘프트웨어를 추가하는 경우에는 그에 대한 보안방책을 작성하여야 합니다.

5) 체계보안방책에 대한 기초개념

여기에서는 보안리눅스에 기초하여 체계의 위임접근조종을 실현하고있는 체계보안방책에 대한 개념을 서술하고있습니다.

(1) 접근조종모형

《붉은별》 봉사기용체계 3.0 에서는 형시행모형과 역할기초의 접근조종모형에 기초하여 위임접근조종을 시행하고있습니다.

① 시행모형

일반적으로 형시행모형은 프로쎄스에 최소한의 권한을 할당하기 위한 모형으로서 프로쎄스에는 령역(domain), 객체에는 형(type)이라는 표제를 붙이고 이 보안표제에 기초하여 접근을 조종합니다. 형시행모형은 개별적인 쏘프트웨어실행에 대한 강력한 조종을 제공합니다.

《붉은별》 봉사기용체계 3.0 에서 리용하고있는 형시행모형은 프로쎄스와 객체에 대한 보안표제로서 한개의 형속성만을 사용합니다. 한개 형이 프로쎄스의 령역으로써 그리고 련관된 객체의 형으로써 사용될수 있습니다. 즉 내부적으로는 령역과 형을 구별하지 않습니다.

다음으로 보안리눅스 형시행모형은 일반적인 형시행모형과 달리 Flask 보안방식에 의해 제공되는 보안클라스정보를 사용합니다. 보안리눅스 형시행모형은 주동체와 객체로 이루어진 보안문맥과 보안클라스에 기초하여 접근결정을 진행합니다. 따라서 형이 같은 객체들을 서로 다른 보안클라스로서 취급할수 있습니다.

또한 일반적인 형시행모형과는 달리 보안리눅스에서는 사용자를 령역과 련관시키지 않습니다. 사용자 관리를 위하여 보안리눅스는 사용자와 령역사이 련계를 지어주는 역할기초의 접근조종모형을 사용합니다.

② 역할기초의 접근조종모형

역할기초의 접근조종은 어떤 자원에 대한 접근권한을 사용자에게 직접 할당하지 않고 주어진 체계환경에서 정의된 역할들에 할당하는 방법으로 체계자원에 대한 접근을 조종합니다.

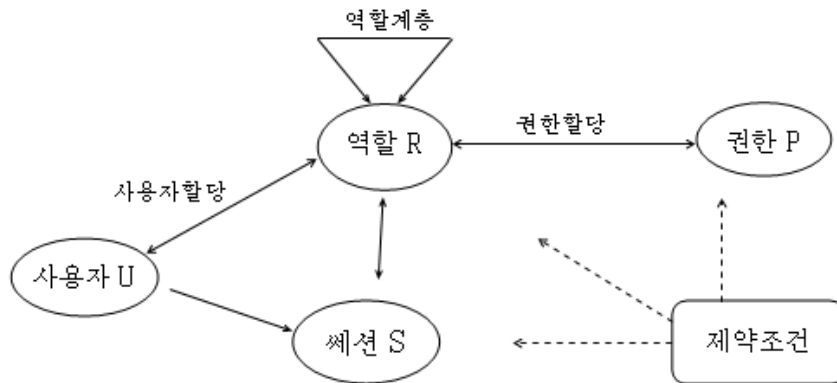



그림 17. 역할기초의 접근조종모형

역할기초의 접근조종모형은 최소권한의 원칙이나 임무분리의 원칙과 같은 보안원칙들을 실행하는데 적합한 모형입니다.

《붉은별》 봉사기용체계 3.0 에서 리용하고있는 역할기초의 접근조종 모형은 매 사용자에게 역할모임을 할당하고 매 역할에 형시행모형에서 규정한 령역모임을 할당하고있습니다.

③ 다중준위 및 다중분류모형(MLS/MCS 모형)모형)

다중준위보안은 벨-라파둘라보안(기밀성)모형에 기초하여 위임접근조종을 실현하고있습니다. 다중준위보안모형에서 모든 주동체들과 객체들은 보안등급을 할당받습니다. 주동체에게 부여되는 보안등급을 인가등급, 정보객체에 주어지는 보안등급을 기밀등급이라고 합니다. 다중분류모형은 다중준위모형에 기초하여 매 주동체와 객체에 그것들이 속하는 분류를 지정함으로써 실현할수 있습니다.

벨-라파둘라보안모형에서는 주동체의 보안준위가 객체의 보안준위보다 높거나 같으며 객체의 모든 분류를 주동체가 포함하고있을 때에만 정보의 읽기를 허가합니다. 또한 객체의 보안준위가 주동체의 보안준위보다 높거나 같으며 주동체의 모든 분류를 객체가 포함하고있을 때에만 정보의 쓰기를 허가합니다.

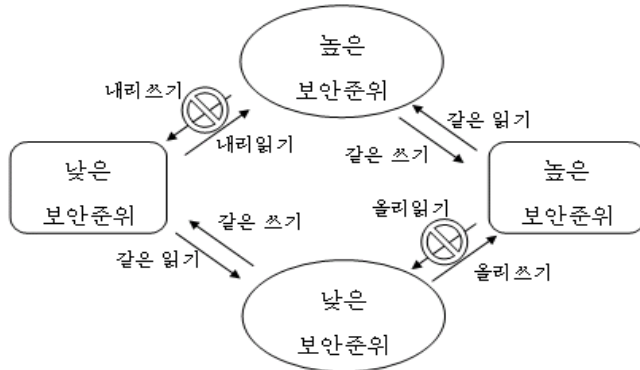



그림 18. 다중준위 및 다중분류 보안모형

《붉은별》 봉사기용체계 3.0 에서는 다중준위 및 다중분류모형에 기초한 접근조종을 시행하지 않습니다.

《붉은별》 봉사기용체계 3.0 에서는 이상의 보안모형들에 기초하여 접근조종을 시행하기 위하여 주동체와 객체들에 보안문맥을 다음과 같은 형식으로 할당합니다.

《사용자명》:《역할》:《령역형》:《다중준위 및 다중분류》

이와 같은 보안문맥에 기초하여 보안방책을 작성합니다.

(2) 체계보안방책 구성화일

《붉은별》 봉사기용체계 3.0 에서 보안관리자는 /etc/selinux 등록부안의 화일들에 대한 접근을 통하여 보안리눅스방책에 대한 관리를 진행합니다.

여기서는 보안리눅스방책이 설치될 때 생성되는 화일들에 대하여 서술합니다. 이 화일들을 리용하여 현재 시행되고있는 보안방책에 기초하여 간단한 설정을 진행할수 있습니다.

① 범용구성화일

보안리눅스방책에 의해 리용되는 일반적인 구성화일들은 다음과 같습니다.

/etc/selinux/config 화일

이 화일은 다음의 변수들을 리용하여 보안방책의 상태를 조종합니다.

SELINUX=enforcing|permissive|disabled

SELINUXTYPE=rss|targeted

SELINUX 변수는 보안방책의 시행방식을 설정합니다. 보안리눅스는 이 변수가 enforcing 으로 설정되면 시행방식으로, permissive 로 설정되면 허가방식으로 동작하며 disabled 로 설정되면 보안리눅스를 시행하지 않게 됩니다.

SELINUXTYPE 변수는 체계기동시에 적재되는 보안방책의 형을 정의합니다. 《붉은별》 봉사기용체계 3.0 에서는 기정으로 rss 형과 targeted 형의 보안방책이 설치됩니다.

기타 구성화일들
/etc/selinux/semanage.conf 화일은 semanage와 semodule지령들에 대한 동작을 조종합니다.
/etc/selinux/restorecond.conf 화일은 정확하지 않은 보안문맥을 가진 응용쏘프트웨어들에 의해 창조될수 있는 화일목록들을 포함합니다. 이와 같은 화일들은 restorecond 대몬에 의하여 자동적으로 보안문맥이 수정되게 됩니다.
/etc/sestatus.conf 화일은 sestatus지령에 의하여 리용됩니다.
/etc/security/sepermit.conf 화일은 보안리눅스가 시행방식으로 동작하는 경우에는 사용자가입을 허가하고 보안리눅스를 사용하지 않는 경우에는 사용자가입을 거부하도록 하는 pam_sepermit.so 모듈에 의해 리용됩니다.

② 방책저장고안의 구성화일들

방책저장고는 /etc/selinux/《방책이름》등록부로 설정되여있습니다. 이 저장고안의 화일들은 semodule이나 semanage지령에 의해 설치되고 갱신됩니다.
modules/active/base.pp 화일
객체클라스들과 접근권한에 대한 선언, 초기 보안식별자(SID)들과 같은 방책부분품들과 모듈을 포함하고있는 기초방책입니다.
modules/active/base.linked 화일
semodule_link를 리용하여 련결되는 모듈들을 포함합니다.
modules/active/commit_num 화일
libsemanage에 의해 리용되는 2진화일입니다.
modules/active/file_contexts.template 화일
이 화일은 모든 모듈들안에 포함되여있는 화일문맥정보들을 포함합니다.
modules/active/file_contexts 화일
이 화일은 /modules/active/file_contexts.template 화일안의 입구점들로부터 생성되며 ./contexts/file/file_contexts 화일로 됩니다. 이 화일은 체계안의 화일과 등록부들이 보안방책에 기초하여 정확히 재표식이 진행되도록 하는데 리용됩니다.
modules/active/homedir_template 화일
이 화일은 /modules/active/file_contexts.template 화일안의 입구점들로부터 생성됩니다. 이 화일은 genhomedircon이나 semanage login, semanage user 지령에 의해 file_contexts.homedirs 화일안에 개별적인 사용자입구점들을 생성하는데 리용됩니다.
/modules/active/file_contexts.homdedirs 화일
이 화일은 사용자등록부가 보안방책에 따라 정확히 재표식되도록 하는데 리용됩니다.
/modules/active/policy.kern 화일

이 화일은 semanage 나 semodule 에 의해 생성되는 2 진 방책화일이며 핵심부에 적재되는 /etc/selinux/《방책이름》/policy 등록부안에 policy.[ver]로 복사됩니다.

/modules/active/seuser.final, seusers 화일

이 화일은 표준 Linux 사용자와 보안리눅스사용자사이 대응관계를 포함하고있습니다. 이 화일은 semodule_package 지령으로 base.pp 를 설치할 때 –s 항목을 리용하는 경우에 설치되게 됩니다. 또한 semanage login 지령에 의해 표준 Linux 사용자에 보안리눅스사용자를 대응시키려고 할 때 갱신되게 됩니다.

/modules/active/users_extra, users_extra.local, users.local 화일

users_extra 화일은 모든 방책에서 앞붙이들을 포함하고있으며 users_extra.local 화일은 semanage user 지령에 의해 생성되는 앞붙이들을 포함하고있습니다.

users.local 화일은 새로운 보안리눅스사용자를 보안방책에 추가하는데 리용됩니다.

/modules/active/booleans.local 화일

이 화일은 semanage boolean 지령에 의해 생성되고 갱신됩니다.

/modules/active/file_contexts.local 화일

이 화일은 semanage fcontext 지령에 의해 생성되고 갱신되며 핵심 보안방책(모듈안에 *.fc 화일)에 포함되여있지 않는 화일과 등록부들에 대한 화일문맥정보를 얻는데 리용됩니다.

/modules/active/interfaces.local 화일

이 화일은 semanage interface 지령에 의해 생성되고 갱신되며 핵심 보안방책(base.conf 화일)에 포함되여있지 않는 망대면부정보를 얻는데 리용됩니다.

/modules/active/nodes.local 화일

이 화일은 semanage node 지령에 의해 생성되고 갱신되며 핵심 보안방책(base.conf 화일)에 포함되여있지 않는 망주소정보들을 얻는데 리용됩니다.

/modules/active/ports.local 화일

이 화일은 semanage port 지령에 의해 생성되고 갱신되며 핵심 보안방책(base.conf 화일)에 포함되여있지 않는 망포구정보를 얻는데 리용됩니다.

/modules/active/modules 등록부

이 등록부는 semodule_package 지령에 의해 묶여진 적재가능한 모듈들을 포함하고있습니다.

③ 보안방책구성화일

seusers 화일

이 화일은 사용자가입 쏘프트웨어에 의해 리용되며 표준 Linux 사용자를 보안리눅스사용자에 대응시킵니다.

/policy/policy.24

이 화일은 보안방책을 시행하기 위하여 핵심부에 적재되는 2 진 보안방책화일이며 checkpolicy 지령이나 semodule 지령에 의해 생성됩니다. 24 는 보안방책화일의 판본을 나타냅니다.

/contexts/customizable_types 화일

이 화일은 setfiles 지령이나 restorecon 지령에 의해 재표식되지 않는 형목록을 포함하고있습니다. 이 지령들은 재표식전에 이 화일을 검사하고 –F 항목이 리용되지 않는경우 목록에서 그 화일들을 배제합니다.

/contexts/default_contexts 화일

이 화일은 사용자프로쎄스(일반적으로 login 응용쏘프트웨어)에 대한 보안문맥설정을 요구하는 보안리눅스관련 응용쏘프트웨어들에 의해 리용됩니다.

/contexts/default_type 화일

이 화일은 newrole 과 같은 보안리눅스관련 응용쏘프트웨어들이 어떤 역할에 대한 기정 령역형을 선택하는데 리용됩니다.

/contexts/failsafe_context 화일

이 화일은 login 프로쎄스가 기정 보안문맥을 결정할수 없을 때 유효한 문맥을 설정함으로써 관리자가 체계에 접근할수 있도록 하는데 리용됩니다.

/contexts/initrc_contexts 화일

이 화일은 체계봉사들을 init 와 같은 보안문맥으로 기동하도록 하는 run_init 지령에 의하여 리용됩니다. 이 화일은 또한 보안리눅스관련 응용쏘프트웨어에 의해서도 리용될수 있습니다.

/contexts/removable_contexts 화일

이 화일은 /contexts/files/media 화일안에서 정의되여있지 않는 제거가능한 장치들에 리용되게 되는 기정표식을 포함하고있습니다.

/contexts/securetty_types 화일

이 화일은 역할이나 준위를 변경할 때 tty 장치를 리용하는 형을 찾기 위하여 newrole 지령에 의해 리용됩니다.

/contexts/files/file_contexts 화일

이 화일은 방책이 갱신될 때 semodule 과 semanage 지령에 의하여 관리되며 사용자가 변경할수 없습니다. 이 화일은 화일체계 전체 혹은 부분을 재표식하기 위하여 여러가지 보안리눅스관련 지령들(setfiles 와 fixfiles, matchpathcon, restorecon)에 의하여 리용됩니다.

/context/files/file_contexts.local 화일

이 화일은 semanage fcontext 지령에 의해 추가되며 국부적으로 정의된 화일들의 보안문맥을 정확히 표식하는데 리용됩니다.

/contexts/files/file_contexts.homedirs 화일

이 화일은 semodule 과 semanage 지령에 의해 관리되며 사용자가 변경할수 없습니다. 이 화일은 genhomedircon 지령에 의해 생성되며 사용자등록부와 화일들에 정확한 보안문맥을 설정하는데 리용됩니다.

/contexts/files/media 화일

이 화일은 어떤 형태의 매체에 보안문맥화일을 대응시키는데 리용됩니다. 만일 화일안에서 media_id 를 찾지 못하는 경우에는 /contexts/removable_contexts 안에 있는 기정문맥이 리용됩니다.

/contexts/users/[seuser_id] 화일

매 화일은 /contexts/default_contexts 화일과 같은 형식을 취하고있으며 보안리눅스 사용자에게 정확한 보안문맥을 할당하는데 리용됩니다.

seuser_id 는 보안리눅스사용자 식별자를 나타냅니다.

2. 체계관리

《붉은별》 봉사기용체계 3.0 에서는 체계관리자역할과 보안관리자역할을 제공하고있습니다.

봉사기관리자가 체계에 가입할 때 관리자에게 기정으로 할당되는 역할은 체계관리자역할입니다. 만일 보안방책과 련관된 과제를 수행하려고 한다면 보안관리자역할로 이행하여야 합니다. 보안관리자역할에로의 이행은 root 사용자에 대한 인증을 요구합니다.

이 장에서는 보안방책이 시행되고있는 환경에서의 봉사기관리방법과 보안방책관리방법을 설명합니다.

1) 체계관리자의 접근권한

① 체계가입

《붉은별》 봉사기용체계 3.0 에서는 봉사기관리자가 사용자식별자와 암호를 가지고 체계에 성공적으로 가입하면 그에게 기정으로 체계관리자역할을 할당합니다.

```
[root@testServer]#id –Z
root:sysadm_r:sysadm_t
```

다음으로 봉사기관리자가 원격관리프로그람(실례로 putty)을 리용하여 체계에 가입하는 경우 접근조종체계는 봉사기관리자에게 일반관리자역할(staff_r)을 할당하게 됩니다. 이 역할로서는 체계관리를 진행할수 없습니다. 따라서 봉사기관리자는 다음과 같은 역할이행지령을 리용하여 체계관리자역할로 이행하여야 합니다.

(putty 를 리용하여 원격으로 가입하는 경우 관리자의 보안문맥)

```
[root@testServer]$id –Z
root:staff_r:staff_t
```

[root@testServer]#newrole –r sysadm_r
암호:
[root@testServer]#id –Z
root:sysadm_r:sysadm_t

봉사기관리자는 이상과 같은 역할을 할당받아야 체계관리를 진행할수 있습니다.

현재 시점에서 봉사기관리자가 보안관리를 진행할 필요가 있는 경우 보안관리자역할로 이행하여야 합니다. 체계관리자역할로부터 보안관리자역할로의 이행은 다음과 같은 지령으로 진행됩니다.

[root@testServer]#newrole –r secadm_r
암호:
[root@testServer]#id –Z
root:secadm_r:secadm_t

② 체계구성 및 봉사대몬관리

봉사기관리자가 체계관리자역할을 할당받은 경우 체계구성과 관련한 설정들을 진행할수 있습니다.

또한 체계관리자는 봉사대몬에 대한 관리를 진행할수 있습니다.

체계관리자는 일반 조작체계에서와 같이 다음의 지령을 리용하여 봉사대몬에 대한 관리를 진행할수 있습니다.

실례 1: 일반적인 체계봉사대몬 관리
#service beam status
beam is starting…
실례 2: run_init 지령을 리용한 체계봉사대몬 관리
#run_init service beam status
permission denied.

다음으로 체계관리자는 체계관리지령들을 실행시킬수 있습니다.

체계관리자가 보안방책과 련관된 지령들을 실행하려는 경우에는 보안관리자역할로 이행하여야 합니다.

2) 체계관리자와 보안관리자의 호상이행

체계관리자와 보안관리자사이의 호상이행을 진행하는데서 보안관리자만의 통과암호를 설정하고 리용함으로써 보안관리자와 체계관리자를 리하였습니다.

Sadm 프로그람을 리용하여 체계관리자에서 보안관리자에로의 가입과 다시 체계관리자로의 이행을진행합니다. 앞에서 서술한 newrole 지령은 sadm 을 통하여 실행되게 됩니다.

(1) 보안관리자의 통과암호 설정

보안관리자의 통과암호는 아래의 지령으로 설정합니다.

sadm -s

(2) 관리자 호상이행

sadm지령을 리용하여 관리자 호상이행을 진행합니다. 아래의 지령을 리용하면 가입한 후 보안관리자로 이행을 진행할수 있습니다.

sadm –r secadm_r

다음 보안관리자의 통과암호를 먼저 확인합니다. 이때 newrole지령이 실행되게 되는데 그러면 체계관리자의 통과암호를 입력하여야 보안관리자로 가입되게 됩니다.

보안관리자에서 체계관리자로 이행하려면

sadm –r sysadm_r

지령을 실행하고 체계관리자의 통과암호를 확인하면 됩니다.

3) 보안관리자의 접근권한

① 보안관리자가입

봉사기관리자가 보안관리자로서의 기능을 실행하려면 다음의 지령을 통하여 보안관리자역할로 이행하여야 합니다.

#newrole –r secadm_r

#id -Z

sysadm_u:secadm_r:secadm_t

다음으로 봉사기관리자가 원격관리프로그람(실례로 putty)을 리용하여 체계에 가입하는 경우 접근조종체계는 봉사기관리자에게 일반관리자역할(staff_r)을 할당하게 됩니다. 이 역할로서는 보안관리를 진행할수 없습니다. 따라서 봉사기관리자는 다음과 같은 역할이행지령을 리용하여 보안관리자역할로 이행하여야 합니다.

(putty를 리용하여 원격으로 가입하는 경우 사용자의 보안문맥)

[root@testServer]$id –Z

root:staff_r:staff_t

[root@testServer]#newrole –r secadm_r

암호:

[root@testServer]#id –Z

root:secadm_r:secadm_t

봉사기관리자는 이상과 같은 역할을 할당받아야 보안관리를 진행할수 있습니다.

현재 시점에서 봉사기관리자가 체계관리를 진행할 필요가 있는 경우 체계관리자역할로 이행하여야 합니다. 보안관리자역할로부터 체계관리자역할로의 이행은 다음과 같은 지령으로 진행됩니다.

[root@testServer]#newrole –r sysadm_r

암호:

[root@testServer]#id –Z
root:sysadm_r:sysadm_t

② 보안구성화일 설정

보안관리자역할을 할당받은 봉사기관리자(보안관리자)는 보안방책과 관련한 설정을 진행할수 있습니다.

보안관리자는 /etc/selinux/config 화일에 대한 쓰기권한을 가지고있습니다.

만일 체계관리자가 이 화일의 내용을 변경하려는 경우 보안방책에 의해 그 조작은 실패하게 됩니다.

또한 보안관리자는 /etc/selinux/《보안방책형》/contexts 등록부안의 화일들의 내용도 변경할수 있습니다.

지령형식은 다음과 같습니다.

semanage {boolean|login|user|port|interface|node|
fcontext|translation} -{l|D} [-n] [-S store]
semanage boolean -{d|m} [-1|-0] -F bool | boolean_file
semanage login -{a|d|m} [-sr] login_name | %groupname
semanage user -{a|d|m} [-LrRP] selinux_name
semanage port -{a|d|m} [-tr] [-p proto] port | port_range
semanage interface -{a|d|m} [-tr] interface_spec
semanage node -{a|d|m} [-tr] [-p prot] [-M mask] address
semanage fcontext -{a|d|m} [-frst] file_spec
semanage permissive -{a|d} type
semanage module -{a|d} policy_package
semanage translation -{a|d|m} [-T] level

여기서 –a, -d, -D 항목은 각각 추가, 삭제, 전체항목 삭제를 나타냅니다.

실례 3: semanage 지령을 리용한 보안관리

# 보안리눅스사용자목록보기
$ semanage user -l
# 사용자 kkh 에 보안리눅스사용자 staff_u 를 대응
$ semanage login -a -s staff_u joe
# kkh 집단에 보안리눅스사용자 user_u 를 대응
$ semanage login -a -s user_u %clerks
# /web 등록부안의 모든 등록부 및 화일들에 대한 화일문맥을 추가(restorecon 에 의해 리용됩니다.)
$ semanage fcontext -a -t httpd_sys_content_t "/web(/.*)?"
# Apache 가 포구 81 에 접속하도록 허가
$ semanage port -a -t http_port_t -p tcp 81
# Apache 를 허가방식 령역으로 변경
$ semanage permissive -a httpd_t

getsebool 과 setsebool 지령

getsebool 지령은 현재 보안리눅스에서 정의된 론리값목록을 보여줍니다.
setsebool 지령은 론리값들의 설정을 변경할수 있습니다.
지령형식은 다음과 같습니다.
#gestsebool [–a] Boolean
#setsebool bool1=val1 bool2=val2…

제2절. 방화벽관리도구(iptables)

여기서는 관리도구를 설치하고 방화벽대몬을 기동중지하며 방화벽규칙을 작성하는 방법에 대하여 서술합니다.

1. 방화벽관리도구의 개요

방화벽관리도구는 방화벽이 설치되여있는 체계에 들어오거나 그 체계를 통하여 전송되거나 그 체계에서 나가는 모든 파케트들에 대하여 방화벽관리자가 작성한 규칙에 따라 핵심부의 netfilter 기능을 리용하여 통과시키거나 파기시키는 것과 같은 처리를 하는 쏘프트웨어입니다.

방화벽관리도구를 리용하여 자기의 콤퓨터와 국부망에 련결된 다른 콤퓨터들을 외부의 접근으로부터 보호할수 있습니다.

《붉은별》 봉사기용체계 3.0 에서는 iptables 를 리용하여 방화벽을 구축하고 있습니다.

방화벽은 표, 사슬, 규칙과 같은 3 개의 오브젝트로 구성됩니다.

매 표들은 여러개의 기정사슬을 포함하고있으며 여러개의 사용자정의사슬도 포함할수 있습니다.

세개의 표에 포함되여있는 기정사슬들은 다음과 같습니다.

- 파케트려과(Filter)
  수신(INPUT), 전송(FORWARD), 송신(OUTPUT)
- 망주소변환(NAT)
  경로선택전(PREROUTING), 송신(OUTPUT), 경로선택 후 (POSTROUTING)
- 파케트변환(Mangle)
  경로선택전(PREROUTING), 수신(INPUT), 전송(FORWARD), 송신 (OUTPUT), 경로선택 후 (POSTROUTING)

매 사슬은 방화벽에 수신되거나 방화벽에서 송신되는 파케트들에 적용할 규칙들을 포함할수 있습니다.

파케트가 사슬을 통과할 때 사슬에 포함되여있는 매개 규칙에 따라 규칙의 조건에 맞는 파케트에 대하여 규칙의 동작을 적용합니다. 규칙의 동작에 따라 파케트는 통과할수도 있고 차단될수도 있습니다.

● **화일목록**

iptables-1.4.9-1.RSS3.i686.rpm
iptables-ipv6-1.4.9-1.RSS3.i686.rpm

2. 방화벽관리도구의 설치

① 설치검사

조종탁에서 다음의 지령을 실행시켜 패키지가 설치되였는가를 검사합니다.

rpm –q iptables

패키지가 설치되여있으면 다음과 같은 통보문이 현시됩니다.

iptables-1.4.9-1.RSS3.i686

② 설치

패키지가 설치되여있지 않은 경우에는 조종탁에서 다음의 지령을 실행시켜 패키지를 설치합니다. 이때 패키지의 설치과정이 현시됩니다.

rpm –ivh iptables-1.4.9-1.RSS3.i686.rpm

3. 사용밥법

1) 방화벽봉사의 시작과 중지

①봉사의 시작상태검사

방화벽대몬의 시작상태를 검사하기 위해서는 콘솔에서 다음의 지령을 실행시킵니다.

service iptables status

대몬이 정확히 기동하고있는 경우에는 방화벽규칙들이 현시됩니다.

실례:

```
#service iptables status
i filter
Chain INPUT (policy ACCEPT)
num target prot opt source destination
1 ACCEPT all – 0.0.0.0/0 0.0.0.0/0 state RELATED,ESTABLISHED
2 ACCEPT icmp – 0.0.0.0/0 0.0.0.0/0
3 ACCEPT all – 0.0.0.0/0 0.0.0.0/0
4 ACCEPT tcp – 0.0.0.0/0 0.0.0.0/0 state NEW tcp dpt:22
5 REJECT all – 0.0.0.0/0 0.0.0.0/0 reject-with icmp-host-prohibited
Chain FORWARD (policy ACCEPT)
num target prot opt source destination
1 ACCEPT all – 0.0.0.0/0 0.0.0.0/0 PHYSDEV match –physdev-is-bridged
2 REJECT all – 0.0.0.0/0 0.0.0.0/0 reject-with icmp-host-prohibited
Chain OUTPUT (policy ACCEPT)
num target prot opt source destination
```

②봉사의 시작

방화벽봉사를 기동시키기 위해서는 다음의 지령을 실행시킵니다.

service iptables start

③봉사의 중지

방화벽봉사를 중지시키기 위해서는 다음의 지령을 실행시킵니다.
이때 체계는 방화벽으로서의 동작을 할수 없게 됩니다.

service iptables stop

④봉사의 재시작

방화벽봉사를 재시작시키기 위해서는 다음의 지령을 실행시킵니다.

service iptables restart

2) 방화벽규칙관리

① 방화벽규칙의 열람

방화벽규칙을 열람하기 위해서는 다음의 지령을 실행시킵니다.

iptables [-t <*table*>] –L [<*chain*>]

표이름을 지정하지 않는 경우에는 기정적으로 filter 표의 규칙들이 현시됩니다. 아래의 모든 지령들에서도 이와 마찬가지로 됩니다.

사슬이름을 지정하지 않는 경우에는 표안의 모든 사슬들에 관하여 규칙들이 현시됩니다.

실례:

```
# iptables -t nat -L PREROUTING
Chain PREROUTING (policy ACCEPT)
target prot opt source destination
```

② 사슬추가

표에 새로운 사슬을 추가하기 위해서는 다음의 지령을 실행시킵니다.

iptables [–t <*table*>] –N <*chain*>

실례:

```
# iptables -t mangle -N samplechain
# iptables -t mangle –L
Chain PREROUTING (policy ACCEPT)
target prot opt source destination
Chain INPUT (policy ACCEPT)
target prot opt source destination
Chain FORWARD (policy ACCEPT)
target prot opt source destination
Chain OUTPUT (policy ACCEPT)
target prot opt source destination
Chain POSTROUTING (policy ACCEPT)
target prot opt source destination
Chain samplechain (0 references)
target prot opt source destination
```

③ 사슬삭제

표에서 사슬을 삭제하기 위해서는 다음의 지령을 실행시킵니다.

iptables [–t <*table*>] –X [<*chain*>]

이때 표에 있는 사용자정의사슬만 삭제할수 있습니다. 사슬이름을 지정하지 않는 경우에는 표안의 모든 사용자정의사슬들이 삭제됩니다.

실례:

```
# iptables -t mangle -X samplechain
# iptables -t mangle –L
Chain PREROUTING (policy ACCEPT)
target prot opt source destination
Chain INPUT (policy ACCEPT)
target prot opt source destination
Chain FORWARD (policy ACCEPT)
target prot opt source destination
Chain OUTPUT (policy ACCEPT)
target prot opt source destination
Chain POSTROUTING (policy ACCEPT)
target prot opt source destination
```

④ 사슬초기화

표에서 사슬의 내용을 초기화 즉 사슬에 포함된 모든 규칙들을 삭제하기 위해서는 다음의 지령을 실행시킵니다.

iptables [–t <*table*>] –F [<*chain*>]

사슬이름을 지정하지 않는 경우에는 표안의 모든 사슬들에 대하여 사슬안의 규칙들이 삭제됩니다.

실례:

```
# iptables –L
Chain INPUT (policy ACCEPT)
target prot opt source destination
ACCEPT all – anywhere anywhere state RELATED,ESTABLISHED
ACCEPT icmp – anywhere anywhere
ACCEPT all – anywhere anywhere
ACCEPT tcp – anywhere anywhere state NEW tcp dpt:ssh
REJECT all – anywhere anywhere reject-with icmp-host-prohibited
Chain FORWARD (policy DROP)
target prot opt source destination
ACCEPT all – anywhere anywhere PHYSDEV match –physdev-is-bridgedREJECT all – anywhere anywhere reject-with icmp-host-prohibited
Chain OUTPUT (policy ACCEPT)
target prot opt source destination

# iptables -F INPUT
# iptables -F FORWARD
# iptables –L
Chain INPUT (policy ACCEPT)
target prot opt source destination
Chain FORWARD (policy DROP)
```

```
target prot opt source destination
Chain OUTPUT (policy ACCEPT)
target prot opt source destination
```

⑤ 사슬방책설정

사슬이 진행할 동작 즉 사슬의 방책을 설정하려는 경우에는 다음의 지령을 실행시킵니다.

iptables [-t <*table*>] –P <*chain*> <*policy*>

사슬방책으로는 ACCEPT, DROP, QUEUE, RETURN 을 줄수 있습니다.

ACCEPT 는 파케트의 허가를 의미하고 DROP 는 파케트의 파기, QUEUE 는 파케트의 대기, RETURN 은 파케트의 되돌리기를 의미합니다.

실례:

```
#iptables –L
Chain INPUT (policy ACCEPT)
target prot opt source destination
Chain FORWARD (policy ACCEPT)
target prot opt source destination
Chain OUTPUT (policy ACCEPT)
target prot opt source destination

#iptables -P FORWARD DROP
#iptables –L
Chain INPUT (policy ACCEPT)
target prot opt source destination
Chain FORWARD (policy DROP)
target prot opt source destination
Chain OUTPUT (policy ACCEPT)
target prot opt source destination
```

⑥ 사슬이름변경

사용자정의사슬의 이름을 변경시키기 위해서는 다음의 지령을 실행시킵니다. 이름이 변경되는 경우에 사슬안의 규칙들은 삭제되지 않습니다.

iptables [-t <*table*>] –E <*oldchain*> <*newchain*>

⑦ 규칙추가

사슬에 새로운 규칙을 추가하기 위해서는 다음의 지령을 실행시킵니다.

iptables [-t <*table*>] –A <*chain*> [-p <*protocol*>] [-s <*address*>[/<*mask*>]] [-d <*address*>[/<*mask*>]] [-i <*name*>] [-o <*name*>] [-j <*target*>]

여기에서 *protocol* 은 규약이름, *address* 는 IP 주소, *mask* 는 마스크, *name* 은 망대면부, *target* 는 방책 또는 사용자정의사슬이름입니다.

아래의 실례는 원천주소가 172.16.1.150 이고 목적주소가 172.16.1.100 이며 규약이 tcp 이고 망장치가 eth0 인 파케트를 접수하며 전달은 접숙하지 않는다는 규칙을 적용하는 실례입니다.

실례:

```
#iptables -A INPUT -p tcp -s 172.16.1.150 -d 172.16.0.100 -i eth0 -j ACCEPT
```

```
# iptables –L
Chain INPUT (policy ACCEPT)
target prot opt source destination
ACCEPT tcp – 172.16.1.150 172.16.0.100
Chain FORWARD (policy DROP)
target prot opt source destination
Chain OUTPUT (policy ACCEPT)
target prot opt source destination
```

⑧ 규칙삽입

사슬의 어떠한 위치에 새로운 규칙을 삽입하기 위해서는 다음의 지령을 실행시킵니다. 삽입할 위치를 지정하지 않는 경우에는 사슬의 첫번째 위치에 규칙이 삽입됩니다.

iptables [-t <*table*>] –I <*chain*> [<*num*>] [-p <*protocol*>] [-s <*address*>[/<*mask*>]] [-d <*address*>[/<*mask*>]] [-i <*name*>] [-o <*name*>] [-j <*target*>]

실례:

```
# iptables –I INPUT 1 -p tcp -s 172.16.1.151 -d 172.16.0.100 -i eth0 -j ACCEPT
# iptables –L
Chain INPUT (policy ACCEPT)
target prot opt source destination
ACCEPT tcp – 172.16.1.151 172.16.0.100
ACCEPT tcp – 172.16.1.150 172.16.0.100
Chain FORWARD (policy DROP)
target prot opt source destination
Chain OUTPUT (policy ACCEPT)
target prot opt source destination
```

⑨ 규칙수정

이미 작성된 규칙의 내용을 변경시키기 위해서는 다음의 지령을 실행시킵니다. 이때 사슬안에서 규칙의 위치를 지정해주어야 합니다.

iptables [-t <*table*>] –R <*chain*> <*num*> [-p <*protocol*>] [-s <*address*>[/<*mask*>]] [-d <*address*>[/<*mask*>]] [-i <*name*>] [-o <*name*>] [-j <*target*>]

추가선택 –R 를 리용하여 규칙을 수정합니다. 실례에서는 *–R INPUT 1* 이라는 추가선택으로 규칙을 수정합니다.

실례:

```
# iptables –R INPUT 1 -p tcp -s 172.16.1.152 -d 172.16.0.100 -i eth0 -j ACCEPT
# iptables –L
Chain INPUT (policy ACCEPT)
target prot opt source destination
ACCEPT tcp – 172.16.1.152 172.16.0.100
ACCEPT tcp – 172.16.1.150 172.16.0.100
Chain FORWARD (policy DROP)
target prot opt source destination
Chain OUTPUT (policy ACCEPT)
target prot opt source destination
```

⑩ 규칙삭제

이미 작성된 규칙을 삭제하기 위해서는 다음의 지령을 실행시킵니다.

다음 지령은 사슬안에서 규칙조건이 일치하는 규칙을 찾아 삭제합니다.

iptables [-t <*table*>] –D <*chain*> [-p <*protocol*>] [-s <*address*>[/<*mask*>]] [-d <*address*>[/<*mask*>]] [-i <*name*>] [-o <*name*>] [-j <*target*>]

실례:

```
# iptables –D INPUT -p tcp -s 172.16.1.150 -d 172.16.0.100 -i eth0 -j ACCEPT
# iptables –L
Chain INPUT (policy ACCEPT)
target prot opt source destination
ACCEPT tcp -- 172.16.1.152 172.16.0.100
Chain FORWARD (policy DROP)
target prot opt source destination
Chain OUTPUT (policy ACCEPT)
target prot opt source destination
```

다음 지령은 사슬안에서 지정한 위치의 규칙을 삭제합니다.

iptables [-t <*table*>] –D <*chain*> <*num*>

실례:

```
# iptables –D INPUT 1
# iptables –L
Chain INPUT (policy ACCEPT)
target prot opt source destination
Chain FORWARD (policy DROP)
target prot opt source destination
Chain OUTPUT (policy ACCEPT)
target prot opt source destination
```

제5장. 기억장치관리

제1절. iSCSI

1. 개요

여기서는 봉사기관리자가 iscsi-initiator-utils 의 사용에서 나서는 문제들과 사용방법에 대하여 서술합니다.

iscsi-initiator-utils-6.2.0.872-10.RSS3 는 《붉은별》 봉사기용체계 3.0 에서 iscsi 기억장치들을 리용하기 위한 쏘프트웨어입니다.

이 쏘프트웨어는 iSCSI 장치들을 탐색하고 거기에 가입하게 하며 open-iscsi 자료기지에 접근하여 관리하게 하는 지령방식도구입니다

봉사기관리자가 아닌 일반 사용자는 이 쏘프트웨어를 리용할수 없습니다.

- 가동환경

iscsi 기억장치를 관리하는 쏘프트웨어로써 설치와 가동환경에는 특별한 요구조건이 없이《붉은별》 봉사기용체계 3.0 이 가동하는 환경이면 되지만 관리대상인 iscsi 기억장치는 필수적입니다.

- 구성관계

쏘프트웨어는 iscsi 장치를 관리하는 부분과 iscsid 대몬을 실행하고 구성화일들을 조작하는 부분으로 구성됩니다.

> **주의**: iscsi장치가 비정상적인 동작을 하거나 중지되는 경우 망련결상태를 감시해보고 대몬이 정확히 동작하는가를 확인해야 합니다.

2. 쏘프트웨어의 설치

《붉은별》 봉사기용체계 3.0 을 설치하면 iscsi-initiator-utils 가 자동적으로 설치됩니다.

또는 iscsi-initiator-utils-6.2.0.872-10.RSS3.i686.rpm 을 수동적으로 설치할수도 있습니다.

콤퓨터의 전원을 켜고《붉은별》 봉사기용체계 3.0 을 기동합니다. 기동 후에 설치판 iscsi-initiator-utils-6.2.0.872-10.RSS3.i686.rpm 가 있는 등록부로 이행합니다.

다음의지령을 입력하면 수동적인 설치가 진행됩니다.

rpm –ivh iscsi-initiator-utils-6.2.0.872-10.RSS3.i686.rpm

덧쓰기하려면 이미 설치된것을 선택항목 –e 를 리용하여 삭제하고 다시 지령을 주거나 –force 선택항목을 함께 주어 덧쓰기 할수 있습니다.

3. 관리방법

1) init 스크립트나 수동적인 기동을 리용하여 iSCSI 를 시작

- 시작

open-iscsi 를 기동시 자동적으로 시작되도록 하자면 다음의 명령을 실행하십시오.

chkconfig --level <levels> open-iscsi on

그리고 기동시 자동적으로 화일체계를 탑재하기 위해서는 /etc/fstab 에 "_netdev"라고 표식된 구획입구점을 가지고있어야 합니다.

아래의 지령은 iscsi 디스크인 sdb 를 탑재합니다.

/dev/sdb /mnt/iscsi ext3 _netdev 0 0

만약 initd 스크립트가 없는 경우에 수동적으로 도구를 시작해야 합니다. 먼저 아래의 지령으로 iSCSI 대몬처리가 시작된 다음 iscsi 모듈을 적재해야 합니다.

modprobe -q iscsi_tcp

- 중지

비정상이 발생하거나 강제로 중지시키려면 Ctrl+C 건을 누릅니다.

2) 자료기지의 조작

iscsiadm 지령을 리용하여 iscsi 장치를 관리할수 있습니다.

iscsiadm 는 iSCSI 대상들을 탐색하고 거기에 가입하게 하며 open-iscsi 자료기지에접근하고 관리하게 하는 지령방식도구입니다.

iscsiadm 도구는 고정자료기지를 관리(갱신, 삭제, 삽입, 질의)하는 지령식도구입니다.

이 도구는 사용자가 iSCSI 마디, 대화접속, 련결, 탐색레코드에서 수행할수 있는 조작들의 모임을 제공합니다.

Iscsiadm 은 해당한 망기판과 주소를 가지고 자료기지의 장치들을 탐색하고 거기에 가입하도록 해줍니다.

이 지령의 –m 선택항목으로 discoverydb 를 지정하면 자료기지에 대한 조작을 진행할수 있습니다.

이때 목적장치의 주소를 인수로 가져야 합니다.

3) 장치의 탐색

iscsiadm 은 탐색에 기정통로를 리용합니다. 이것은 지정한 iface 를 리용하지 않습니다. 그리하여 offload 기판을 리용하고있다면 탐색목적을 위하여 장치에 구별되는 망을 련결하여야 합니다.
호환성으로 인하여 iscsiadm 을 실행하여 탐색할 때 iface.transport 를 위하여 tcp 를 리용하고있는 /var/lib/iscsi/ifaces 에서 결합부를 조사하고 탐색한 주소를 련결하여 그 iface 를 통하여 가입합니다. 이 처리는 리용하려는 결합부에 넘겨주어 무시할수 있습니다. cxgb3i 와 bnx2i 를 가지고있는 offload 의 경우 전송이 tcp 가 아니므로 요구됩니다.
실례로 두개의 결합부를 정하였지만 하나를 리용하고 싶다면 --interface/-I 인수를 리용할수 있습니다.

iscsiadm -m discoverydb -t st -p ip:port -I iface1 --discover -P 1

결합부를 정의하였지만 iface 에 대화접속을 련결하지 않는 낡은 방식을 원한다면 그때 특수한 iface "default"를 리용할수 있습니다.

iscsiadm -m discoverydb -t st -p ip:port -I default --discover -P 1

그리고 /var/lib/iscsi/ifaces 에 어떤 결합부도 정의하지 않았고 iscsiadm 에 아무것도 넘겨주지 않는다면 iscsiadm 의 실행은 기정방식으로 처리하는데 여기서는 망부분체계가 리용할 장치를 결정합니다.
후에 특수한 장치와 iface 의 련결을 제거하려면 다음의 지령을 실행하십시오.
iscsiadm -m node -T my_target -I iface0 --op=delete

장치의 지정한 주소를 위하여 이것을 하기 위하여 다음과 같이 실행합니다.

iscsiadm -m node -T my_target -p ip:port -I iface0 --op=delete

iface0 의 모든 련결들을 제거하고 싶다면 다음과 같이 실행합니다.

iscsiadm -m node -I iface0 --op=delete

그리고 같은 론리의 장치들을 위하여 때때로 주소를 리용하여 제거하는것이 유익합니다.
iscsiadm -m node -p ip:port -I iface0 --op=delete

iSCSI 는 3 개의 discovery 형 즉 SendTargets, SLP 와 iSNS 을 지원합니다.
SendTargets 는 매 iSCSI 목표들이 사용가능한 목표들의 목록을 initiator 에 보내도록 하는 기초적인 iSCSI 규약입니다.

SLP 선택적으로 어떤 iSCSI 목표가 봉사위치규약(SLP)를 리용하여 사용가능한 목표를 통지할수 있게 합니다.

initiator 는 SLP 질문에 직접 대답하든가 혹은 별개의 도구를 리용하여 사용가능한 목표들에 대한 정보를 얻을수 있습니다.

iSNS (Internet Storage Name Service : 인터네트 기억장치 이름봉사)는 대규모 망안에 있는 기억장치기록권에 대한 정보를 기록합니다. iSNS 를 리용하려면 탐색할 iSNS 봉사기의 주소와 포구를 선택하여야합니다.

fw 여러 NIC 들과 체계들은 기동시에 리용될수 있는 소형 iSCSI initiator 를 포함하고있습니다. 기동에 리용되는 값을 얻기 위하여 fw 선택항목을 리용할수 있습니다. fw 탐색에서는 마디나 탐색 DB 에 고정레코드를 보관하지 않는데 그것은 그 값들이 체계나 NIC 의 자원에 보관되기때문입니다.

fw 탐색을 수행하는것은 다른 탐색방법과 같이 portal 를 표시합니다. CHAP 값과 같은 다른 설정들과 initiator 설정들을 보기 위하여 node 방식에서 iscsiadm -m fw"을 실행하십시오.

iscsiadm 은 iSNS (isns) 나 SendTargets(st)탐색형을 지원합니다. SLP 실현은 개발중에 있습니다.

4) 대면부의 선택

iscsiadm 지령의 –I 선택항목을 리용하여 조작에 리용할 iscsi 대면부를 지정합니다. iSCSI 대면부(iface)들은 /var/lib/iscsi/ifaces 에 정의됩니다. iface 는 iface 구성화일의 이름입니다.

하드웨어 iSCSI(qla4xxx)일 때 iface 에는 하드웨어주소(iface.hwaddress =포구의 MAC 주소)와 구동쏘프트웨어/trans-port_name (iface.transport_name)이 있어야 합니다. 쏘프트웨어 iSCSI 일 때 iface 에는 하드웨어주소(iface.hwaddress) 나 망층 대면부이름 (iface.net_ifacename)과 구동쏘프트웨어/transport_name 이 있어야 합니다.

사용가능한 구동쏘프트웨어/iscsi_transports 는 tcp (TCP/IP 쏘프트웨어 iSCSI), iser (무한대역쏘프트웨어 iSCSI) 혹은 qla4xxx (Qlogic 4XXXX HBAs)입니다. hwaddress 는 MAC 주소이거나 쏘프트웨어 iSCSI 일 때는 특수한 값 "default"일수 있는데 이것은 initiator 가 특정한 하드웨어자원에 대화접속을 련결하지 말고 대신 망이나 무한대역층이 무엇을 하겠는지 결심하도록 하게 할것을 지시합니다. 기정동작으로 ifaceconfig 를 생성할 필요는 없습니다. 만약 iface 를 지정하지 않으면 기정동작을 리용합니다.

우에서 언급한 iface 이름은 기정입니다. 그외에 ccxgb3i, bnx2i 와 iser 의 3 개가 있는데 이것들은 특정한 카드에 대화접속을 련결하지 않지만 cxgb3i, bnx2i 나 iser 전송에 대화접속을 련결합니다.

탐색방식에서 -I/--interface 실체를 여러번 지정하여 다중대면부를 지정할수 있습니다.

실례로

"iscsiadm -m discoverydb -t st -p ip:port -I iface0 -I iface2 --discover"는 마디 db 를 설정하여 두개 대면부로 대화접속을 창조할 레코드들을 생성하게 합니다.

node 방식에서는 오직 한개 대면부만을 지정할수 있습니다.

이 선택항목은 discovery, node 와 iface 방식에서 유효합니다.

5) 마디

iscsiadm --mode node 지령은 현재 존재하는 모든 마디레코드들을 현시합니다.

--mode node 선택항목을 리용하여 리용하여 마디들에 대한 조작을 진행할수 있습니다.

마디레코드들에로의 가입과 탈퇴, 삭제를 수행할수 있습니다.

6) 대화접속

대화접속은 iscsiadm 지령에 --login 을 리용하여 진행합니다.

--mode 와 --targetname, --portal 를 지정하여 목적장치에로의 대화접속을 진행합니다.

접속탈퇴를 진행하려고 할 때는 --logout 를 리용합니다.

4. 대몬관리

iscsi 장치를 관리하기 위해서는 먼저 iscsid 라는 관리대몬을 시작하여야 합니다.

이 대몬은 iscsid 는 iSCSI 규약의 조종경로와 일부 관리기능들을 실현합니다.

실례로 대몬을 변하지 않는 iSCSI 자료기지의 내용에 기초하여 기동시 자동적으로 탐색을 다시 시작하도록 구성할수 있습니다.

/etc/iscsi/iscsid.conf, /etc/iscsi/initiatorname.iscsi, /etc/iscsi/nodes 화일들을 구성화일로서 소유하고있습니다.

이 iscsid 지령을 리용하여 이 구성화일들의 정보를 변경시킬수 있습니다.

대몬의 시작방법에 대하여서는 이미 3)의 (1)에서 서술하였습니다.

제2절. mdadm

여기서는《붉은별》 봉사기용체계 3.0 에서 mdadm 를 설치리용하기 위한 방법을 설명합니다

1. 화일구성과 설치

- 화일구성

mdadm 은 md 에 기초한 쏘프트웨어 RAID 를 실현하는 도구입니다.

《붉은별》 봉사기용체계 3.0 에서 mdadm-3.1.3-1.RSS3.i686.rpm 패키지를 설치합니다.

mdadm 패키지는 RAID 관리도구인 mdadm 과 설정화일, 도움말로 이루어집니다.

- 설치

mdadm 은 《붉은별》 봉사기용체계 3.0 이 설치될 때 자동적으로 설치됩 니다.

CD 를 리용하여 설치를 진행하는 경우에는 먼저 CD 구동기에《붉은별》 봉사기용체계 3.0 CD 를 넣고 탑재를 시켜야 합니다.

mount /dev/cdrom /mnt/cdrom

패키지들이 들어있는 등록부에서 설치하려는 패키지들이 있는가를 확인합니다. 확인이 끝나면 설치를 시작합니다.

mdadm-3.1.3-1.RSS3.i686.rpm 패키지를 설치합니다.

rpm –ivh mdadm-3.1.3-1.RSS3.i686.rpm

2. 쏘프트웨어의 사용

mdadm 은 조작탁에서 리용합니다.

1) RAID 배렬의 창조

명령행에 다음과 같은 형식으로 입력합니다.

mdadm --create **RAID 장치이름** --raid-devices=**부분장치개수** --raid-devices [부분장치개수] -n [능동장치개수] -x [여유장치개수] -l [RAID 준위] **부분장치 1 ... 부분장치 n**

표 6. 유효한 RAID 준위

RAID 준위
Linear
raid0, 0, stripe
raid1, 1, mirror
raid4, 4
raid5, 5
raid6, 6
raid10, 10
multipath, mp

Faulty
Container

표 7. 유효한 배치형식

배치형식	**유효한 RAID 준위**
left-asymmetric, la	RAID5, RAID6
left-symmetric, ls	RAID5, RAID6
right-asymmetric, ra	RAID5, RAID6
right-symmetric, rs	RAID5, RAID6
party-first	RAID5, RAID6
party-last	RAID5, RAID6
ddf-zero-restart	RAID5, RAID6
ddf-N-restart	RAID5, RAID6
ddf-N-continue	RAID5, RAID6
left-asymmetric-6	RAID6
left-symmetric-6	RAID6
right-asymmetric-6	RAID6
right-symmetric-6	RAID6
party-first-6	RAID6
write-transient, wt	Faulty
read-transient, rt	Faulty
write-persistent, wp	Faulty
read-persistent, rp	Faulty
write-all	Faulty
read-fixable, rf	Faulty
Clear	Faulty
Flush	Faulty
None	Faulty

실례: mdadm --create /dev/md0 --level=1 --raid-devices=2 /dev/hda1 /dev/sdc1

실례에 대한 설명: /dev/hda1 과 /dev/sdc1 로 구성되는 RAID1 배렬장치인 /dev/md0 을 창조합니다.

2) RAID 배렬의 관리-부분장치의 추가 및 삭제

명령행에 다음과 같은 형식으로 입력합니다.

mdadm **RAID 장치이름 [추가선택항목 1 부분장치 1] … [추가선택항목 n 부분장치 n]**

- 부분장치의 추가

추가선택항목형식: -a(또는 –add) **부분장치**
설명: 배렬에 **부분장치**를 추가합니다.
- 부분장치의 삭제
추가선택항목형식: -r(또는 –remove) **부분장치**
설명: 배렬로부터 **부분장치**를 삭제합니다.
- 부분장치를 고장으로 설정
추가선택항목형식: -f(또는 –faulty) **부분장치**
설명: 배렬에서 **부분장치**를 고장으로 설정합니다.

실례: mdadm /dev/md0 --add /dev/sda1 --fail /dev/sdb1 --remove /dev/sdb1
실례에 대한 설명: RAID 배렬 /dev/md0 에 먼저 /dev/sda1 를 부분장치로 추가하고 배렬에 있던 /dev/sdb1 부분장치를 faulty 로 설정한 다음 그것을 배렬로부터 삭제합니다.

3) RAID 배렬의 구동

명령행에 다음과 같은 형식으로 입력합니다.
mdadm --assemble –scan
그러면 창조된 RAID 배렬을 검출하여 자동적으로 구동됩니다.

4) RAID 배렬의 중지

구동중인 **RAID 장치**를 중지하기 위하여 명령행에 다음과 같은 형식으로 입력합니다.
mdadm --stop(또는 –S) **RAID 장치**

실례: mddadm --stop /dev/md0
실례에 대한 설명: /dev/md0 배렬을 중지시킵니다.

제3절. dmraid

1. 쏘프트웨어 구성

여기서는 《붉은별》 봉사기용체계 3.0 에서 dmraid 를 설치리용하기 위한 방법을 설명합니다.
dmraid 는 Device-Mapper 를 리용하여 ATARAID 와 같은 RAID 장치들을 장치특정의 구동쏘프트웨어가 없이도 리용하도록 지원하는 도구입니다.
dmraid 는 Device Mapper 를 리용하여 특정한 장치구동쏘프트웨어가 없이도 RAID 를 지원합니다.

– 쏘프트웨어 구성

dmraid 패키지는 RAID 장치의 검색과 능동 및 비능동화를 실현하는 도구인 dmraid와 이를 위한 서고들, 도움말로 이루어집니다.

dmraid의 패키지이름은 dmraid-1.0.0-rc16.10-RSS3.i686.rpm 입니다.

– 쏘프트웨어 설치

dmraid는 《붉은별》 봉사기용체계 3.0이 설치될 때 자동적으로 설치됩니다.

CD를 리용하여 설치를 진행하는 경우에는 먼저 CD구동기에 《붉은별》 봉사기용체계 3.0 CD를 넣고 탑재를 시켜야 합니다.

mount /dev/cdrom /mnt/cdrom

패키지들이 들어있는 등록부에서 설치하려는 패키지들이 있는가를 확인합니다. 확인이 끝나면 설치를 시작합니다.

2. 사용방법

dmraid는 조작탁에서 리용합니다.

1) RAID 모임의 능동화

명령형식: dmraid –ay

탑재된 모든 쏘프트웨어 RAID 모임을 능동화합니다.

2) RAID 모임의 비능동화

명령형식: dmraid –an

모든 혹은 특정한 쏘프트웨어 RAID 모임을 비능동으로 합니다.

3) RAID 모임의 현시

명령형식: dmraid –l

사용가능한 RAID 장치들의 목록을 보여줍니다.

4) RAID 모임의 삭제

명령형식: dmraid –x [RAID 모임]

한개 혹은 모든 쏘프트웨어 RAID 장치들을 삭제합니다.

5) RAID 모임의 재구축

명령형식: dmraid –x [RAID 모임]

어떤 구동기가 고장나고 새로운 구동기가 추가된 경우 이 명령을 리용하여 RAID 모임을 재구축합니다.

6) 블로크장치현시

명령형식: dmraid –b

모든 블로크장치들을 속성과 함께 현시합니다.

7) RAID 장치현시

명령형식: dmraid –r

모든 RAID 장치들을 그의 형식, RAID 준위, 리용된 분구수등과 함께 현시합니다.

8) 메타자료현시

명령형식: dmraid –n

모든 메타자료들을 제작회사특정의 형식으로 현시합니다.

제4절. LVM2

1. 쏘프트웨어 구성과 설치

여기서는 기억장치를 관리하는 관리자들을 위하여 론리기록권관리도구인 lvm2-2.02.83-3.RSS3.i686.rpm 의사용밥법에 대하여 설명하고있습니다.

따라서 기억장치 즉 하드디스크구동기와 구획 등에 대한 기억장치에 대한 지식을 가진 사용자들을 대상으로 하고있습니다

－ 쏘프트웨어 구성

이 쏘프트웨어는 론리기록권(LV)과 물리기록권(PV), 물리기록권들의 집단(VG)의 관리부분들로 구성됩니다.

LV 관리는 LV 의 창조와 제거, 속성변경, 크기변경, 이름변경 등을 진행하는 부분입니다.

PV 관리는 PV 의 창조와 제거, 속성변경, 블로크장치조사를 진행하는 부분입니다.

VG 관리는 VG 의 창조와 제거, 속성변경, PV 추가, 블로크장치조사, VG 들의 결합과 분리, 여벌복사 등을 진행하는 부분입니다.

－ 쏘프트웨어 설치

LVM2 을 사용하기 위해서는 우선《붉은별》 봉사기용체계 3.0 이 설치되여있어야 합니다.

《붉은별》 봉사기용체계 3.0 을 먼저 기동합니다.

다음으로 LVM2 은 lvm2-2.02.83-3.RSS3.i686.rpm 패키지를 설치하여야 합니다.

조종탁상에서

rpm -ivh lvm2-2.02.83-3.RSS3.i686.rpm

을 입력하여 설치를 진행합니다.

설치가 완료되면 완료되였다는 통보문이 현시됩니다.

－ 봉사의 시작

LVM2 을 리용하여 물리기록권들을 가상화화여 론리기록권들로서 리용하기 위해서는 먼저 콤퓨터에 1 개이상의 블로크장치가 있어야 합니다.

먼저 물리기록권이라는 표식을 블로크장치에 달아주어야 합니다.

다음으로 이 물리기록권들로서 기록권집단을 창조해주어야 합니다.

다음으로 창조된 기록권집단에서 편의에 따라 론리기록권들을 창조하여 일반 하드디스크나 기억기처럼 사용합니다.

론리기록권들의 창조시에 선형입출력방식인가 병렬입출력방식인가 등 여러가지 설정을 진행함으로써 론리기록권의 기록방식을 개선하고 자료입출력속도를 개선할수 있습니다.

－ 봉사의 중지

LVM2 을 리용하여 기억장치들에 대한 관리를 중지하려는 경우에는 현재 탑재된 론리기록권들에 대한 해제로써 수행합니다.

해제는 umount 지령을 리용하여 진행합니다.

만일 현재 탑재된 론리기록권에 대한 입출력처리가 진행중인 경우에는 자료의 파괴가 일어날수 있으므로 이러한 조작들을 모두 정상완료하고 탑재를 해제하여야 합니다.

2. 사용방법

LVM2 은 콤퓨터에 설치되여있는 여러개의 블로크장치들(하드디스크나 구획들)을 가상화하여 여러개의 기록권집단을 창조하고 이 기록권집단상에서 론리기록권들을 사용자의 편의에 따라 창조함으로써 사용자들이 물리적인 기억기들에 대한 설치나 해제 또는 구획변경과 같은 많은 시간과 품이드는 조작들을 진행함이 없이 안전한 자료복사와 처리를 진행하도록 하는 편의쏘프트웨어입니다.

LVM2 의 사용은 다음의 단계를 거쳐서 진행되게 됩니다.

① 물리기록권들의 창조

② 기록권집단의 창조

③ 론리기록권을 창조

우의 단계를 거쳐 론리기록권을 창조한 후에는 일반적인 디스크를 탑재하는 것과 같은 방법으로 그 론리기록권을 리용할수 있습니다.
이때 알아야 할것은 론리기록권자체가 한개의 하드디스크처럼 동작한다는것입니다.

1) 물리기록권들에 대한 관리방법

이 절에서는 물리기록권들을 관리하기 위한 여러가지 지령들의 사용방법에 대하여 서술합니다.

① 물리기록권의 창조

LVM2 을 사용하기 위해서는 우선 물리기록권을 창조해야 합니다.

－ 물리기록권의 구획형설정

물리기록권을 창조하기 위해서는 먼저 물리기록권의 구획형을 설정해야 합니다.

만일 전체 디스크장치를 물리기록권으로 사용하고있다면 그 디스크에는 구획표가 없어야 합니다.

DOS 디스크구획구조에서는 fdisk 나 cfdisk 지령 혹은 그와 같은것들을 리용하여 구획 ID 를 0x8e 로 설정하여야 합니다.

전체 디스크장치들에서 구획표들만을 지우기 함으로서 디스크의 전체 자료들을 효과적으로 제거하여야 합니다.

아래의 지령으로 첫 분구를 령으로 초기화함으로서 현존 구획표를 효과적으로 제거할수 있습니다.

dd if=/dev/zero of=PhysicalVolume bs=512 count=1

－ 물리기록권들의 초기화

pvcreate 지령을 리용하여 물리기록권으로 리용되는 블로크장치를 초기화합니다.

초기화는 화일체계의 형식화와 류사합니다.

아래의 지령은 /dev/sda1, /dev/sdb1, 그리고 /dev/sdc1 를 LVM 물리기록권들로 리용하기 위하여 초기합니다.

pvcreate -/dev/sda1 -/dev/sdb1 -/dev/sdc1

－ 블로크장치들에 대한 조사

현재 콤퓨터에 접속되여있는 블로크장치들에 대한 조사를 먼저 진행하여 물리기록권으로 창조할 장치들을 먼저 알아볼수 있습니다.

lvmdiskscan 지령을 사용하여 물리기록권으로 사용할수 있는 블로크장치들을 조사할수 있습니다.

② 물리기록권들의 표시

현재 창조된 물리기록권들에 대한 정보를 보기 위해서 pvs, pvdisplay, pvscan 지령을 리용할수 있습니다.

pvs 지령은 물리기록권당 한행씩 구성가능한 형식으로 물리기록권정보를 제공합니다.

pvs 지령은 다양한 형식조종을 제공하며 스크립트화에 유리합니다.

pvdisplay 지령은 매 물리기록권에 대한 상세한 다중행출력을 제공합니다.

이 지령은 고정된 형식으로 물리적속성(크기, 령역, 기록권집단 등)을 현시합니다.

pvscan 지령은 물리기록권을 찾기 위하여 체계우에서 지원되는 LVM 블로크장치들을 모두 조사합니다.

매 지령들은 선택항목을 가지고있지 않습니다.

③ 물리기록권우에서의 할당금지

pvchange 지령으로 1 개 혹은 그 이상의 물리기록권우에서 물리령역들을 할당하는것을 금지할수 있습니다.

이것은 디스크오유가 있어가 물리기록권을 제거하려고 할 때 필요할수 있습니다.

아래의 지령은 /dev/sdk1 에서 물리령역들의 할당을 금지합니다.

Pvchange –x n -/dev/sdk1

또한 pvchange 지령의 –xy 인수를 리용하여 이미 금지하였던것에서의 할당을 허용할수도 있습니다.

④ 물리기록권의 크기조절

어떤 리유로 하위블로크장치의 크기를 변경할 필요가 있다면 pvresize 지령을 사용하여 새 크기로 LVM 을 갱신하여야 합니다.

LVM 이 그 물리기록권을 사용할 때 이 명령을 실행할수 있습니다.

⑤ 물리기록권들의 제거

어떤 장치가 더 이상 LVM 에 필요없는 경우에는 pvremove 지령을 리용하여 LVM 표식자를 제거할수 있습니다.

pvremove 지령은 빈 물리기록권우에서 LVM 메타자료들을 0 으로 지우기합니다.

만일 제거하려는 물리기록권이 현재 어떤 블로크집단이 한 성원이라면 vgreduce 지령을 리용하여 물리기록권을 그 블로크집단에서 제거하여야 합니다.

pvremove -/dev/ram15

제거가 성과적으로 진행된 경우에 성공하였다는 통보문이 현시됩니다.

2) 기록권집단관리

이 절에서는 기록권관리를 진행하는데 리용할수 있는 지령들에 대하여 설명합니다.

① 기록권집단의 창조

한개 혹은 그 이상의 물리기록권들로 기록권집단을 창조하기 위하여서는 vgcreate 지령을 사용하여야 합니다.

vgcreate 지령은 이름을 가지고 새로운 기록권집단을 창조하며 여기에 적어도 한개의 물리기록권을 추가합니다.

아래의 지령은 물리기록권들이 /dev/sdd1 과 /dev/sde1 을 포함하는 기록권집단을 vg1 이라는 이름으로 합니다.

vgcreate vg1 -/dev/sdd1 -/dev/sde1

물리기록권들이 블로크집단을 창조하는데 리용될 때 그의 디스크공간은 보통 4MB 령역으로 분할되게 됩니다.

기정령역크기가 적합치 않을 때에는 vgcreate 지령의 –s 선택항목을 가지고 령역크기를 지정할수 있습니다.

또한 vgcreate 지령에서 –p 와 –l 인수를 리용하여 기록권집단의 물리기록권수와 론리기록권수의 한계를 정할수 있습니다.

보통 기록권집단은 같은 물리기록권우에 병렬입출력기록권들을 배치하지 않는다는것과 같은 명백한 규칙들에 따라 물리령역들을 할당합니다.

이것이 normal 할당방책입니다. vgcreate 지령의 –alloc 인수를 리용하여 할당방책을 contigious, anywhere 혹은 cling 중의 하나로 지정할수 있습니다.

contigious 방책은 새로운 령역들이 현존하는 령역들에 린접할것을 요구합니다.

만약 할당요구를 만족시킬만할 빈 령역이 충분히 있어도 normal 방책은 그 령역들을 리용하지 않지만 anywhere 방책은 두개의 병렬입출력기록권들을 같은 물리기록권우에 배치하는것으로 하여 성능을 떨어뜨릴수 있다고 해도 그 령역들을 리용합니다.

cling 방책은 새로운 령역들을 론리기록권의 현재 령역들이 들어있는 같은 물리기록권우에 배치합니다.

이 방책들은 vgchange 지령으로 변경할수 있습니다.

일반적으로 normal 이 아닌 할당방책들은 비표준인 령역할당을 지정할 필요가 있는 특수한 경우에만 사용하게 됩니다.

LVM 기록권집단들과 하위론리기록권들은 아래의 배치와 같이 /dev 등록부안의 장치특수화일등록부나무에 포함됩니다.

/dev/vg/lv/

실례로 두개의 기록권집단들인 myvg1, myvg2 들과 매 집단들에 3 개의 론리기록권들인 lvo1, lvo2, lvo3 을 창조한다면 이것은 6 개의 장치특수화일들을 창조하게 됩니다.

/dev/myvg1/lv01
/dev/myvg1/lv02
/dev/myvg1/lv03
/dev/myvg2/lv01
/dev/myvg2/lv02
/dev/myvg2/lv03

LVM 의 최대장치크기는 64bit CPU 우에서 8Exabyte 입니다.

② 클라스터환경에서 기록권집단의 창조

클라스터환경에서 기록권집단들은 단일마디에서와 같이 vgcreate 지령으로 창조합니다.

일반적으로 공유기억장치들우에서 CLVM 으로 창조된 기록권집단들은 공유기억장치에 접근하는 모든 콤퓨터들에 다 보이게 됩니다.

그러나 vgcreate 지령의 –c n 을 리용하여 클라스터안에서 한개 마디에게만 보이는 국부적인 기록권집단들을 창조할수도 있습니다.

아래의 지령은 클라스터환경에서 집행될 때 지령이 집행되는 마디에만 한정되는 기록권집단을 창조합니다.

이 지령은 국부기록권집단의 이름은 vg1 로 하며 여기에는 물리기록권들인 /dev/sdd1 와 /dev/sde1 가 포함됩니다.

vgcreate –c n vg1 -/dev/sdd1 -/dev/sde1

현재 존재하는 기록권집단이 국부적인가 아니면 클라스터화되였는가 하는것을 vgchange 지령의 –c 선택항목으로 변경할수 있습니다.

또한 vgs 지령으로 현재 기록권집단이 클라스터화된 기록권집단인가 아닌가를 검사할수 있습니다.

이 지령은 기록권집단이 클라스터화되였으면 c 속성을 현시합니다.

③ 기록권집단에 물리기록권들을 추가

현재 존재하는 기록권집단에 물리기록권들을 추가하기 위하여서는 vgextend 지령을 리용합니다.

vgextend 지령은 한개 혹은 그이상의 빈 물리기록권들을 추가하여 기록권집단의 용량을 증가시킵니다.

아래의 지령은 물리기록권 /dev/sdf1 을 기록권집단 vg1 에 추가합니다.

vgextend vg1 /dev/sdf1

④ 기록권집단의 표시

현재 어떤 기록권집단들이 존재하며 그속성들이 어떤가를 보기 위하여 vgdisplay 와 vgs 지령을 사용할수 있습니다.

vgscan 지령은 기록권집단안의 모든 디스크들을 조사하고 LVM 고속완충기억기화일을 재구축하며 또한 기록권집단들을 현시합니다.

vgs 지령은 구성가능한 형식으로 한개 기록권을 한행에 표시하면서 이 기록권에 대한 정보들을 제공합니다.

vgdisplay 지령은 기록권집단속성들(크기, 령역수, 물리기록권수 등)을 고정된 형식으로 현시합니다.

⑤ 기록권집단에서 고속완충기억기화일구축을 위하여 디스크들을 조사하는 방법

vgscan 지령은 LVM 물리기록권들과 기록권집단들에 대한 체계조사시 지원되는 모든 디스크장치들을 조사합니다.

vgscan 지령은 /etc/lvm/.cache 화일에 LVM 고속완충기억기를 구축하며 이 화일은 현재 LVM 장치들의 목록을 유지보존합니다.

LVM 은 체계기동시와 함께 당신이 vgcreate 지령을 집행할 때나 LVM 이 오유를 검출하였을 때와 같은 LVM 조작시에 vgscan 지령을 자동적으로 실행합니다.

하드웨어구성을 변경하였을 때 vgscan 지령을 수동적으로 실행하여 체계기동시에 주어지지 않았던 새로운 장치가 체계에 보이도록 만들수 있습니다.

⑥ 기록권집단에서 물리기록권들의 제거

기록권집단에서 리용하지 않는 물리기록권들을 제거하기 위해서는 vgreduce 지령을 리용합니다.

vgreduce 지령은 한개 혹은 그이상의 빈 물리기록권들을 제거하여 기록권집단의 용량의 축소합니다.

물리기록권을 기록권집단에서 제거하기전에 먼저 pvdisplay 지령을 리용하여 물리기록권이 론리기록권들에게 리용되지 않는다는것을 확인하여야 합니다.

만약 물리기록권들이 아직 리용되고있다면 pvmove 지령을 리용하여 자료를 다른 물리기록권으로 옮겨야 합니다.

형식: vgreduce 물리기록권이름

⑦ 기록권집단의 속성변경

vgchange 지령을 리용하여 현재 존재하는 기록권집단의 여러가지 기록권집단 속성들을 변경시킬수 있습니다.

실례:아래의 지령은 기록권집단 vg00 의 최대론리기록권수를 128 로 변경합니다.

vgchange –l 128 -/dev/vg00

⑧ 기록권집단의 활성화 및 비활성화

기록권집단을 창조할 때 창조된 기록권집단은 기정적으로 능동화됩니다.

이것은 그 집단안의 론리기록권들에 접근할수 있으며 그것들을 변경할수 있다는것을 의미합니다.

그러나 기록권집단을 비능동화하여 핵심부가 모르게 하여야 할 여러가지 경우가 있을수 있습니다.

기록권집단을 비능동화 혹은 능동화하기 위하여서는 vgchange 지령의 –a(--available)인수를 리용합니다.

실례:아래의 지령은 기록권집단 my_volume_group 을 비능동화합니다.

vgchange –a n my_volume_group

⑨ 기록권집단의 제거

어떠한 론리기록권도 가지지 않는 기록권집단을 제거하기 위하여서는 vgremove 지령을 리용합니다.

형식: vgremove 기록권집단이름

⑩ 기록권집단의 분리와 결합

lvm 은 기록권집단의 물리기록권들을 분리하여 새로운 기록권집단을 창조하기 위하여 vgsplit 지령을 리용합니다.

론리기록권들은 기록권집단들사이에서 분리할수 없습니다.

또한 2 개의 기록권집단들을 하나의 기록권집단으로 결합하기 위하여서 vgmerge 지령을 리용합니다.

두 기록권의 물리령역크기가 같고 물리기록권 및 론리기록권 합계들이 목적기록권집단의 한계에 맞아 들어갑니다면 비능동 원천기록권집단을 능동이거나 비능동인 목적기록권집단으로 결합할수 있습니다.

⑪ 기록권집단의 이름변경 및 다른체계에로의 이동

기록권집단의 이름을 변경하기 위해서 vgrename 지령을 리용합니다.

전체 LVM 기록권집단을 다른 체계에로 옮길수도 있습니다.
기록권집단을 옮길 때에는 vgexport 와 vgimport 지령을 리용하여야 합니다.
vgexport 지령은 비능동기록권집단을 체계가 접근불가능하게 만듬으로서 그 집단의 물리기록권들을 분리해낼수 있게 합니다.
vgimport 지령은 vgexport 지령이 그 집단을 비능동으로 만든 후 기계에서 다시 접근가능하게 합니다.
기록권집단을 한 체계에서 다른 체계에로 옮기려면 아래의 걸음들을 수행하여야 합니다.

- 그어떤 사용자도 기록권집단안의 능동기록권우의 화일들에 접근하고있지 않다는것을 확인하여야 합니다. 그다음 론리기록권들을 탑재해제하여야 합니다.
- vgchange 지령의 –a n 인수를 리용하여 기록권집단을 비능동으로 표식함으로서 기록권집단에 대한 그 어떤 동작도 금지하도록 합니다.
- vgexport 지령을 리용하여 기록권집단을 반출합니다. 이것은 제거하려고 하는 기록권집단에 대한 체계의 접근을 금지합니다.

기록권집단을 반출한 후, 아래의 실례에서 보여주는바와 같이 물리기록권은 반출된 기록권집단안에 있는것으로 표시됩니다.

```
[root@tng3-1]# pvscan
  PV -/dev/sda1    is in exported VG myvg [17.15 GB -/ 7.15 GB free]
  PV -/dev/sdc1    is in exported VG myvg [17.15 GB -/ 15.15 GB free]
  PV -/dev/sdd1   is in exported VG myvg [17.15 GB -/ 15.15 GB free]
  -...
```

체계가 다음번에 전원끄기될 때 그 기록권집단을 구성하는 디스크들을 뽑아서 새 체계에 련결할수 있습니다.

- 디스크들에 새 체계에 련결되였을 때 vgimport 지령을 리용하여 기록권집단을 반입함으로서 새 체계에서 접근가능하게 만듭니다.
- vgchange 지령의 –a y 인수로 기록권집단을 능동화합니다.
- 화일체계를 탑재하여 사용할수 있게 만듭니다.

이밖에도 기록권집단관리를 편리하게 하기 위하여 기록권집단등록부와 론리기록권특수화일을 재창조하기 위한 vgmknodes 지령을 리용할수 있습니다.

3) 론리기록권관리

이 절에서는 론리기록권을 관리하기 위한 여러가지 지령들에 대하여 설명합니다.

① 론리기록권의 창조

론리기록권을 창조하기 위해

서는 lvcreate 지령을 리용합니다.
Lvcreate 지령을 사용하여 선형기록권, 병렬입출력기록권, 대칭복제기록권을 창조할수 있습니다.
만일 론리기록권의 이름을 지정하지 않는 경우 기정이름 lvo1#가 리용되며 #는 론리기록권의 내부번호로 됩니다.

– 선형기록권의 창조

론리기록권을 창조할 때 론리기록권은 기록권집단으로부터 물리기록권들의 빈 령역들을 할당받게 됩니다.
보통 론리기록권은 하위물리기록권우에서 사용가능한 임의의 공간을 리용합니다.
론리기록권의 변경은 물리기록권의 공간해방과 재할당을 진행하도록 합니다.
아래의 지령은 기록권집단 vg1 에서 10GB 크기의 론리기록권을 창조합니다.

```
lvcreate --L 10G vg1
```

아래의 지령은 기록권집단 testvg 안에 testlv 라는 이름으로 1500MB 크기의 선형론리기록권을 창조하며 블로크장치 /dev/testvg/testlv 를 창조합니다.

```
lvcreate --L1500 --n testlv testvg
```

아래의 지령은 기록권집단 vg0 안의 빈 령역을 가지고 gfslv 라는 이름으로 50GB 크기의 론리기록권을 창조합니다.

```
lvcreate --L 50G --n gfslv vg0
```

lvcreate 지령의 –l 파라메터를 리용하여 론리기록권의 크기를 령역단위로 지정할수 있습니다.
아래의 지령은 기록권집단 testvo1 의 총공간의 60%를 리용하는 론리기록권을 mylv 라는 이름으로 창조합니다.

```
lvcreate --l 60%VG --n mylv testvg
```

전체 기록권집단을 리용하는 론리기록권을 창조하는 다른 방법은 vgdisplay 지령으로 “Total PE”크기를 찾아 그 결과를 lvcreate 지령의 입력으로 리용하는것입니다.
아래의 지령은 testvg 라는 기록권집단을 통채로 리용하는 mylv 라는 론리기록권을 창조합니다.

```
# vgdisplay testvg -| grep -"Total PE"
Total PE              10230
# lvcreate --l 10230 testvg --n mylv
```

– 병렬입출력기록권의 창조

다량의 순차적인 읽기와 쓰기를 위하여 병렬입출력론리기록권을 창조하는것은 자료입출력효률을 개선할수 있습니다.

당신이 LVM 론리기록권들에 자료를 쓰기할 때 화일체계는 하위물리기록권들사이에 자료를 배치합니다.

병렬입출력론리기록권을 창조하여 물리기록권들에 자료를 쓰는 방식을 조종할수 있습니다.

대용량자료의 읽기와 쓰기에서 이것은 자료입출력의 효률의 개선할수 있습니다.

병렬입출력은 미리 결정된 수의 물리기록권들에 원형방식으로 자료를 쓰기하여 성능을 개선합니다.

병렬입출력으로 하여 입출력은 병행으로 진행되게 될수 있습니다.

일부 경우에 이것은 병렬입출력에 매번 물리기록권을 추가할 때마다 거의 선형적인 성능향상을 이룩하게 합니다.

병렬입출력론리기록권에서 자료묶음의 크기는 령역의 크기를 초과할수 없습니다.

병렬입출력론리기록권은 첫번째 모임의 끝에 다른 장치모임을 련결하여 확장할수 있습니다.

병렬입출력론리기록권을 확장하기 위하여서는 기록권집단이 병렬입출력을 지원하도록 구성된 하위물리기록권들에 충분한 빈공간이 있어야 합니다.

실례로 만약 전체 기록권집단을 리용하는 2 중병렬입출력을 가지고있다면 한개의 물리기록권을 기록권집단에 추가하는것으로서는 병렬입출력을 확장할수 없습니다.

대신 기록권집단에 최소한 2 개의 물리기록권들을 추가하여야 합니다.

병렬입출력론리기록권을 창조할 때 lvcreate 지령의 –i 파라메터를 가지고 병렬입출력수를 지정할수 있습니다.

이것은 론리기록권에서 얼마나 많은 물리기록권들이 병렬입출력되겠는가를 지정합니다.

병렬입출력수는 (--alloc anywhere 인수가 리용되지 않는다면)기록권집단의 물리기록권수보다 클수 없습니다.

만약 병렬입출력기록권을 구성하는 하위물리장치들의 크기가 서로 다르다면 병렬입출력기록권의 최대크기는 하위장치들중에서 가장 작은 크기로 확정됩니다.

아래의 지령은 2 개의 물리기록권으로 64KB 단위의 병렬입출력론리기록권을 창조합니다.

이 론리기록권의 크기는 50GB 이며 이름은 gfslv 로서 기록권집단 vg0 에서 할당됩니

다.

```
lvcreate --L 50G --i2 --I64 --n gfslv vg0
```

선형기록권에서처럼 병렬입출력으로 리용하는 물리기록권의 령역수를 지정할수 있습니다.

아래의 지령은 물리기록권 testvg 에서 stripelv 라는 이름으로 2 개의 물리기록권으로 병렬로 입출력하는 크기가 100 개 령역인 병렬입출력기록권을 창조합니다.

이 병렬입출력기록권은 /dev/sda1 의 0-50, /dev/sdb1 의 50-100 의 분구들을 리용합니다.

```
# lvcreate --l 100 --i2 --nstripelv testvg -/dev/sda1:0-50 -/dev/sdb1:50-100
  Using default stripesize 64.00 KB
  Logical volume -"stripelv" created
```

– 대칭복제기록권의 창조

대칭복제는 서로 다른 장치들에 자료의 동일한 복사본들을 보존하는것입니다.

자료가 어떤 장치에 씌여질 때 이 자료는 두번째 장치에도 씌여져 대칭복제됩니다.

이것은 장치고장에 대한 보호를 제공하여 줍니다.

대칭복제에서 한쪽 가지가 고장났을 때 론리기록권은 선형기록권으로 되며 그때에도 접근할수 있습니다.

대칭복제론리기록권을 창조하였을 때 LVM 은 한쪽 하위물리기록권에 씌여지는 자료가 다른쪽 물리기록권에 대칭복제시킵니다.

LVM 대칭복제는 복사되는 장치들을 보통 512KB 의 크기를 가지는 구역들로 분할합니다.

LVM 은 어느 구역이 대칭복제(들)와 일치되고있는가를 관리하는데 리용 하는 리력화일를 보관합니다.

이 리력화일은 디스크에 보관될수 있으며 그 경우 재기동 후에도 계속 존재하며 또는 기억기에 보관할수도 있습니다.

대칭복제기록권을 창조할 때 lvcreate 지령의 –m 파라메터로 자료복사본의 개수를 지정할수 있습니다.

-m1 을 지정하면 1 개의 대칭복제 즉 화일체계에 두개 복사본 즉 선형론리기록권 + 한개의 복사본을 만든다.

류사하게 -m2 을 지정하면 2 개의 대칭복제본을 창조하며 화일체계에 3 개 복사본을 만든다.

아래의 지령은 단일대칭복제본으로 구성된 대칭복제론리기록권을 창조합니다.
기록권의 크기는 50GB 이며 이름은 mirrorlv 로서 기록권집단 vg0 에서 할당됩니다.

```
lvcreate --L 50G --m1 --n mirrorlv vg0
```

LVM 대칭복제본은 복제될 장치를 보통 크기가 512KB 인 구역들로 분할합니다.
lvcreate 지령의 –R 파라메터를 리용하여 구역크기를 MB 단위로 지정할수 있습니다.
또한 lvm.conf 화일의 mirror_region_size 설정을 편집하여 기정구역크기를 변경할수 있습니다.
주의할점은 클라스터하부구조의 제한으로하여 1.5TB 보다 큰 클라스터대칭복제본들은 512KB 의 기정구역크기로 창조할수 없다는것입니다.
아래의 지령은 구역크기가 2MB 인 대칭복제기록권을 창조합니다.

```
lvcreate --m1 --L 2T --R 2 --n mirror vol_group
```

– 대칭복제기록권구성의 변경

lvconvert 지령을 리용하여 론리기록권을 대칭복제기록권으로부터 선형기록권으로 혹은 선형기록권으로부터 대칭복제기록권으로 변환할수 있습니다.
론리기록권을 대칭복제기록권으로 변환할 때 우선 현재 존재하는 기록권의 대칭복제다리를 창조하여야 합니다.
이것은 기록권집단이 대칭복제다리와 대칭복제로그를 위한 장치와 공간을 가지고있어야 한다는것을 의미합니다.
만약 대칭복제본의 어떤 다리를 잃는 경우 LVM 은 그 기록권을 선형기록권으로 변환하여 당신이 대칭복제여분이 없이 기록권에 계속 접근하도록 합니다.
다리를 회복한 후에 lvconvert 지령을 리용하여 대칭복제본을 회복할수 있습니다.
아래의 지령은 선형론리기록권 vg00/lvol1 을 대칭복제론리기록권으로 변환합니다.

```
lvconvert --m1 vg00/lvol1
```

아래의 지령은 대칭복제론리기록권 vg00/lvol1 을 선형론리기록권으로 변환합니다.

```
lvconvert --m0 vg00/lvol1
```

② 고정된 장치번호들

장치번호 및 부번호들은 모듈적재시에 동적으로 할당됩니다. 일부 응용쏘프트웨어들은 블로크장치가 항상 같은 장치(주및부)번호를 할당하여야 정확히 동작합니다.

이것을 lvcreate 지령과 lvchange 지령에서 아래의 파라메터들을 리용하여 지정할수 있습니다.

```
--persistent y ---major major ---minor minor
```

다른 장치에 이미 동적으로 할당되지 않은 번호를 쓰기 위하여 부번호를 큰 수로 리용합니다.

③ 론리기록권의 크기변경

론리기록권의 크기를 줄이기 위하여서는 lvreduce 지령을 리용합니다. 만약 론리기록권이 화일체계를 포함하고있다면 먼저 화일체계의 크기를 줄여 론리기록권이 항상 화일체계만큼은 크게 되도록 하여야 합니다.

아래의 지령은 기록권집단 vg00 의 론리기록권 lvol1 의 크기를 3 개의 론리령역으로 축소합니다.

```
lvreduce --l --3 vg00/lvol1
```

④ 론리기록권의 파라메터변경

론리기록권의 파라메터를 변경하기 위하여서는 lvchange 지령을 리용합니다.

lvchange 지령을 리용하여 론리기록권들을 능동화 및 비능동화할수도 있습니다.

어떤 기록권집단안의 모든 론리기록권들을 동시에 능동화 혹은 비능동화하기위하여서는 vgchange 지령을 리용합니다.

아래의 지령은 기록권집단 vg00 의 기록권 lvol1 에 대한 권한을 읽기전용으로 변경합니다.

```
lvchange --pr vg00/lvol1
```

⑤ 론리기록권의 이름변경

현재 존재하는 론리기록권의 이름을 변경하기 위하여 lvrename 지령을 리용합니다.

아래의 두 지령은 기록권집단 vg02 의 론리기록권 lvold 의 이름을 lvnew 로 바꿉니다.

```
lvrename -/dev/vg02/lvold -/dev/vg02/lvnew

lvrename vg02 lvold lvnew
```

⑥ 론리기록권의 제거와 현시

현재 비능동인 론리기록권을 제거하기 위하여 lvremove 지령을 리용합니다.
만약 론리기록권이 현재 탑재되였다면 제거하기전에 탑재해제하여야 합니다.
또한 클라스터환경에서는 론리기록권을 제거하기전에 비능동화하여야 합니다.
아래의 지령은 론리기록권 /dev/testvg/testlv 를 기록권집단 testvg 로부터 제거합니다.
이 경우 론리기록권이 비능동화되지 않는다는데 주의하여야 합니다.

```
[root@tng3-1 lvm]# lvremove -/dev/testvg/testlv
Do you really want to remove active logical volume -"testlv"? [y/n]: y
  Logical volume -"testlv" successfully removed
```

lvchange –an 지령으로 기록권을 제거하기전에 그것을 정확히 비능동화할수 있으며 그때 능동인 론리기록권을 제거하겠는가를 확인하는 재촉문이 현시되지 않습니다.

LVM 론리기록권들의 속성을 현시하는데 리용할수 있는 지령들은 3 가지 즉 lvs, lvdisplay, 그리고 lvscan 입니다.
lvs 지령은 구성가능한 형식은 한행에 한개 론리기록권씩 정보를 제공합니다.
lvs 지령은 풍부한 형식화조종을 제공하며 스크립트화에 유용합니다.
lvdisplay 지령은 론리기록권속성(크기, 배치, 그리고 대응 등)들을 고정된 형식으로 현시합니다.
아래의 지령은 vg00 의 lvol2 의 속성들을 보여줍니다.

```
lvdisplay --v -/dev/vg00/lvol2
```

lvscan 지령은 아래의 실례에서 처럼 체계안의 모든 론리기록권들을 조사하여 그것들을 렬거합니다.

```
# lvscan
 ACTIVE                   -'/dev/vg0/gfslv' [1.46 GB] inherit
```

⑦ 론리기록권의 확장

론리기록권의 크기를 증가시키기 위하여서는 lvextend 지령을 리용합니다.

론리기록권을 확장한 다음 그와 련관된 화일체계의 크기를 증가하여 맞출 필요가 있습니다.

론리기록권을 확장할 때 기록권을 얼마나 확장하겠는가 혹은 확장한 후 얼마만한 크기가 되게 하겠는가 하는것을 지적할수도 있습니다.

아래의 지령은 론리기록권 /dev/myvg/homvol 을 12GB 로 확장합니다.

```
# lvextend --L12G -/dev/myvg/homevol
lvextend --- extending logical volume -"/dev/myvg/homevol" to 12 GB
lvextend --- doing automatic backup of volume group -"myvg"
lvextend --- logical volume -"/dev/myvg/homevol" successfully extended
```

아래의 지령은 론리기록권 /dev/myvg/homevol 에 1GB 를 더합니다.

```
# lvextend --L+1G -/dev/myvg/homevol
lvextend --- extending logical volume -"/dev/myvg/homevol" to 13 GB
lvextend --- doing automatic backup of volume group -"myvg"
lvextend --- logical volume -"/dev/myvg/homevol" successfully extended
```

lvcreate 지령에서와 같이 lvextend 지령에서 –l 파라메터를 리용하여 론리기록권의 크기를 얼마만큼 증가하겠는가 하는 령역개수를 지정할수 습니다.

⑧ 병렬입출력기록권의 확장

병렬입출력론리기록권의 크기를 증가시키기 위하여서는 병렬입출력을 지원하는 기록권집단을 구성하는 하위 물리기록권들에 충분한 빈공간이 있어야 합니다.

실례로전체 기록권집단을 리용하는 2 중병렬입출력을 가지고있는 경우 한개의 단일물리기록권을 기록권집단에 추가하여서는 병렬입출력의 확장이 허용될수 없습니다.

그대신 적어도 2 개의 물리기록권들을 기록권집단에 추가하여야 합니다.

실례로 아래의 vgs 지령에서 보여준바와 같이 2 개의 하위물리기록권들로 구성된 기록권집단 vg 를 고찰합니다.

```
# vgs
  VG   #PV #LV #SN Attr   VSize   VFree
  vg     2   0   0 wz--n- 271.31G 271.31G
```

기록권집단의 전체 공간을 리용하여 병렬입출력을 창조할수 있습니다.

```
# lvcreate --n stripe1 --L 271.31G --i 2 vg
  Using default stripesize 64.00 KB
  Rounding up size to full physical extent 271.31 GB
  Logical volume -"stripe1" created
# lvs --a --o +devices
  LV      VG   Attr   LSize   Origin Snap%  Move Log Copy%  Devices
  stripe1 vg   --wi-a- 271.31G                               -/dev/sda1(0),/dev/sdb1(0)
```

주의할것은 이제는 기록권집단에 빈공간이 더는 없다는것입니다.

```
# vgs
  VG   #PV #LV #SN Attr   VSize   VFree
  vg     2   1   0 wz--n- 271.31G    0
```

아래의 지령이 기록권집단에 또다른 물리기록권을 추가함으로서 135G 의 추가적인 공간이 생기게 되였습니다.

```
# vgextend vg -/dev/sdc1
  Volume group -"vg" successfully extended
# vgs
  VG   #PV #LV #SN Attr   VSize   VFree
  vg     3   1   0 wz--n- 406.97G 135.66G
```

이 시점에서 병렬입출력론리기록권을 기록권집단의 최대크기에로 확장할수 없습니다. 그것은 자료의 병렬입출력을 위하여서는 2 개의 하위장치들이 필요하기때문입니다.

```
# lvextend vg/stripe1 --L 406G
  Using stripesize of last segment 64.00 KB
  Extending logical volume stripe1 to 406.00 GB
  Insufficient suitable allocatable extents for logical volume stripe1: 34480
more required
```

병렬입출력론리기록권을 확장하기 위하여서는 다른 물리기록권을 추가한 다음에 론리기록권을 확장합니다.

이러한 실례로 2 개의 물리기록권들을 기록권집단에 추가한 다음에 론리기록권을 기록권집단의 최대크기에로 확장할수는것을 들수 있습니다.

```
# vgextend vg -/dev/sdd1
  Volume group -"vg" successfully extended
# vgs
  VG   #PV #LV #SN Attr   VSize   VFree
  vg     4   1   0 wz--n- 542.62G 271.31G
# lvextend vg/stripe1 --L 542G
  Using stripesize of last segment 64.00 KB
  Extending logical volume stripe1 to 542.00 GB
  Logical volume stripe1 successfully resized
```

병렬입출력론리기록권을 확장하기에 충분한 하위물리장치들을 가지고있지 못하고있는 경우 확장된것이 병렬입출력이 아니여서 성능이 저하된다고 하여도 일없다면 강제로 기록권을 확장할수도 있습니다.

론리기록권에 공간을 추가할 때 기정조작은 현존하는 론리기록권의 마지막 토막과 같은 병렬입출력파라메터를 리용하는것이지만 이 파라메터들을 무시할수도 있습니다.

아래의 실례는 초기에 lvextend 지령이 실패한 후 현존하는 병렬입출력론리기록권이 나머지 빈공간을 리용하도록 확장합니다.

```
# lvextend vg/stripe1 --L 406G
  Using stripesize of last segment 64.00 KB
  Extending logical volume stripe1 to 406.00 GB
  Insufficient suitable allocatable extents for logical volume stripe1: 34480
more required
# lvextend --i1 --l+100%FREE vg/stripe1
```

⑨ 론리기록권들의 크기축소

론리기록권의 크기를 줄이기 위하여 먼저 화일체계를 탑재해제합니다.
그다음 lvreduce 지령으로 기록권을 축소합니다.
기록권을 축소한 다음 화일체계를 탑재합니다.

주의할점은 기록권 그 자체를 축소하기전에 화일체계 혹은 기록권에 존재하는 자료의 크기를 줄이는것이 중요합니다.

왜냐하면 기록권의 크기를 줄임으로 하여 그 기록권안의 자료가 파괴될수 있기때문입니다.

제6장. 봉사기관리

이 장에서는《붉은별》 봉사기용체계 3.0에 포함된 여러가지 봉사기설정들에 대하여 설명합니다.

제1절. 조선어망령역이름체계《KDNS 3.0》

1. 조선어망령역이름체계의 개요

조선어망령역이름체계 《KDNS 3.0》(이하 KDNS이라고 함)은 《붉은별》 봉사기용체계 3.0에서 이전의 망령역이름봉사체계에서 사용할수 없었던 조선어망령역이름봉사를 실현하게 합니다.

조선어망령역이름체계《KDNS 3.0》은 사용자들이 조선어망령역이름을 리용하여 홈페지열람을 할수 있도록 하였으며 이름봉사기관리에서 편리한 조선어환경과 설정정보에 대한 보안기능을 제공하고있습니다.

조선어망령역이름체계는 《붉은별》2.0(봉사기용체계)에서 제공하고있는 조선어망령역이름체계의 기능을 더욱 향상시켜 사용자들과 봉사기관리자들에게 보다 편리한 조선어망령역이름리용환경을 제공하고 이름봉사기의 보안기능을 강화하는것을 기본목적으로 합니다.

용어 및 략어

BIND(Berkeley Internet Name Domain) : 이름봉사기에 설치되는 쏘프트웨어

DNS(Domain Name System) : 망령역이름체계

ACE(ascii-compatible encoding) : ASCII문자로 변환하는 부호화방식

KDN(Korean domain name) : 조선어망령역이름

Kdnkit.rpm : 조선어망령역이름을 ASCII문자로 부호화하는 실행프로그람

2. 조선어망령역이름체계의 설치와 해제

1) 쏘프트웨어 구성관계

KDNS3.0은 아래의 7개의 rpm실행화일들로 구성됩니다.

bind-9.7.0-5.P2.RSS3.1.i386.rpm
bind-libs-9.7.0-5.P2.RSS3.1.i386.rpm
bind-utils-9.7.0-5.P2.RSS3.1.i386.rpm
bind-devel-9.7.0-5.P2.RSS3.1.i386.rpm
bind-chroot-9.7.0-5.P2.RSS3.1.i386.rpm
bind-sdb-9.7.0-5.P2.RSS3.1.i386.rpm
kdnkit-1.0-1.i386.rpm

2) 설치방법

지령해석기를 기동시킵니다.

① 다음의 순서로 rpm화일들을 설치합니다.

```
# cd 지령으로 rpm화일들이 있는 위치로 이동합니다.
# rpm -ivh --force bind-libs-9.7.0-5.P2.RSS3.1.i386.rpm
# rpm -ivh --force bind-9.7.0-5.P2.RSS3.1.i386.rpm
# rpm -ivh --force bind-utils-9.7.0-5.P2.RSS3.1.i386.rpm
# rpm -ivh --force bind-chroot-9.7.0-5.P2.RSS3.1.i386.rpm
# rpm -ivh --force bind-sdb-9.7.0-5.P2.RSS3.1.i386.rpm
# rpm -ivh --force kdnkit-1.0-1.i386.rpm
```

② 《KDNS 3.0》을 해제하려면 다음과 같이 진행합니다. 먼저 named 대몬을 중지시킵니다.

```
# service named stop
# rpm -e kdnkit-1.0-1.i386.rpm
# rpm -e bind-sdb-9.7.0-5.P2.RSS3.1.i386.rpm
# rpm -e bind-chroot-9.7.0-5.P2.RSS3.1.i386.rpm
# rpm -e bind-utils-9.7.0-5.P2.RSS3.1.i386.rpm
# rpm -e bind-9.7.0-5.P2.RSS3.1.i386.rpm
# rpm -e bind-libs-9.7.0-5.P2.RSS3.1.i386.rpm
```

3. 조선어망령역이름체계의 작업절차

이 장에서 《KDNS 3.0》리용방법에 대하여 설명합니다.

조선어망령역이름을 설정하고 봉사기를 재시작하면 모든 설정에서 조선어로 입력된 내용들이 모두 아스키문자로 변환됩니다.

1) 시작과 중지

KDNS는 체계가 기동하면서 자동으로 시작합니다.

만약 시작하지 않았다면 아래와 같이 합니다.

① 시작

```
#service named start
```

혹은

```
#/etc/init.d/named start
```

② 재시작

```
#service named restart
```

혹은

```
#/etc/init.d/named restart
```

③ 중지

```
# service named stop
```

2) 조선어망령역이름체계 의 설정

해당한 령역화일들을 본문편집기로 편집하여 리용할수 있습니다.

수동설정

- 먼저 DNS봉사기를 설정하여야 합니다. 설정화일은 /etc/resolv.conf 화일입니다.

```
nameserver 172.16.200.83
```

- named구성화일은 /etc/namedkp.conf 화일입니다.

실례:

```
// namedkp.conf
//
options {
    listen-on port 53 { 172.16.200.83; };
    listen-on-v6 port 53 { ::1; };
    directory           "/var/named";
```

```
    dump-file           "/var/named/data/cache_dump.db";
 statistics-file "/var/named/data/named_stats.txt";
 memstatistics-file "/var/named/data/named_mem_stats.txt";
//  allow-query { localhost; };
    recursion yes;

    dnssec-enable yes;
    dnssec-validation yes;
    dnssec-lookaside auto;

    bindkeys-file "/etc/named.iscdlv.key";
};

logging {
 channel default_debug {
 file "data/named.run";
 severity dynamic;
 };
};

zone "." IN {
    type hint;
    file "named.ca";
};

zone "kcc.inf.kp" IN {
    type master;
    file "kcc.inf.kp.db";
    allow-update { none; };
};

zone "내나라.조선" IN {
    type master;
    file "내나라.조선.db";
    allow-update { none; };
};

zone "83.200.16.172.in-addr.arpa" IN {
    type master;
    file "83.200.16.172.db";
    allow-update { none; };
};

include "/etc/named.rfc1912.zones";
```

- /var/named/masters 등록부에 “내나라.조선.db” “kcc.inf.kp.db”과 그의 역방향령역이름인 “83.200.16.172.db”의 zone화일을 설정합니다.

· “내나라.조선.db”zone화일의 실례:

```
$TTL 1D
@ IN SOA @ rname.invalid. (
                                        0        ; serial
                                        1D       ; refresh
                                        1H       ; retry
                                        1W       ; expire
                                        3H )     ; minimum
    NS      kdns.내나라.조선.
kdns        A       172.16.200.83
www         A       10.76.1.2
```

· “83.200.16.172.db”zone화일의 실례:

```
$TTL 1D
@ IN SOA @ rname.invalid. (
                                        0        ; serial
                                        1D       ; refresh
                                        1H       ; retry
                                        1W       ; expire
                                        3H )     ; minimum
   NS       kdns.내나라.조선.
   PTR kdns.내나라.조선.
```

· “kcc.inf.kp.db”zone화일의 실례:

```
$TTL 1D
@ IN SOA @ rname.invalid. (
                                        0        ; serial
                                        1D       ; refresh
                                        1H       ; retry
                                        1W       ; expire
                                        3H )     ; minimum
    NS      kdns.내나라.조선.
kdns        A       172.16.200.83
```

3) 조선어망령역이름

· dig 지령

```
[root@bom rpm]# dig www.내나라.조선
;; 응답을 받았습니다.;
;; ->>머리부<<- 형태: QUERY, 상태: NOERROR, id: 44316
;; 기발들: qr aa rd ra; 질문: 1, 응답: 1, 관할: 1, 추가: 1

;; 질문 구역:
;www.내나라.조선. IN A

;; 응답 구역:
```

```
www.내나라.조선. 38400 IN A 10.76.1.2

;; 관할 구역:
내나라.조선. 38400 IN NS kdns.내나라.조선.
;; 추가 구역:
kdns.내나라.조선. 38400 IN A 172.16.200.83

;; 질문시간: 6msec
;; 봉사기: 172.16.200.45#53(172.16.200.45)
;; 시간: Thu Dec 18 09:34:00 2008/12/18
;; 통보문크기 rcvd: 78

[root@bom rpm]#
[root@bom rpm]# dig -x 172.16.200.83
;; 응답을 받았습니다.;
;; ->>머리부<<- 형태: QUERY, 상태: NOERROR, id: 45392
;; 기발들: qr aa rd ra; 질문: 1, 응답: 1, 관할: 1, 추가: 1

;; 질문 구역:
;83.200.16.172.in-addr.arpa. IN PTR

;; 응답 구역:
83.200.16.172.in-addr.arpa. 86400 IN PTR kdns.내나라.조선.

;; 관할 구역:
83.200.16.172.in-addr.arpa. 86400 IN NS kdns.내나라.조선.

;; 추가 구역:
kdns.내나라.조선. 86400 IN A 172.16.200.83

;; 질문시간: 90msec
;; 봉사기: 172.16.200.45#53(172.16.200.45)
;; 시간: Thu Dec 18 09:34:00 2008/12/18
;; 통보문크기 rcvd: 78

[root@bom rpm]#
```

· host지령

```
[root@bom rpm]# host -a www.내나라.조선
"www.내나라.조선"를 찾고있습니다.
;; ->>머리부<<- 형태: QUERY, 상태: NOERROR, id: 44316
;; 기발들: qr aa rd ra; 질문: 1, 응답: 1, 관할: 1, 추가: 1

;; 질문 구역:
;www.내나라.조선. IN A
```

```
;; 응답 구역:
www.내나라.조선. 38400 IN A 172.16.200.83

;; 관할 구역:
내나라.조선. 38400 IN NS www.내나라.조선.

;; 추가 구역:
www.내나라.조선. 86400 IN A 172.16.200.83

 "172.16.200.45#53" 으로부터 3 ms 내에 103 bytes 를 받았습니다.
[root@bom rpm]#
[root@bom rpm]# host -a 172.16.200.83
 "83.200.16.172.in-addr.arpa"를 찾고있습니다.
;; ->>머리부<<- 형태: QUERY, 상태: NOERROR, id: 45392
;; 기발들: qr aa rd ra; 질문: 1, 응답: 1, 관할: 1, 추가: 1

;; 질문 구역:
;83.200.16.172.in-addr.arpa. IN PTR

;; 응답 구역:
83.200.16.172.in-addr.arpa. 86400 IN PTR kdns.내나라.조선.

;; 관할 구역:
200.16.172.in-addr.arpa. 86400 IN NS kdns.내나라.조선.

;; 추가 구역:
kdns.내나라.조선. 86400 IN A 172.16.200.83

 "172.16.200.83#53" 으로부터 2 ms 내에 100 bytes 를 받았습니다.
[root@bom rpm]#
```

4) 조선어망령역이름 부호화

- 부호화

조선어로 작성된 망령역이름설정화일을 ASCII문자로 작성된 화일로 변환하는 지령입니다.

· 화일부호화

#kdnconv -i UTF-8 namedkp.conf > namedkp.conf1

-i : 입력코드모임 선택항목.

UTF-8: 실지 입력코드모임.

namedkp.conf: 변환하려는 화일이름

namedkp.conf1: 변환된 화일이름

· 문자렬부호화

#kdnconv

국가망   //변환하려는 조선어문자렬을 입력합니다.

xn--o39a10a76y //결과가 출력됩니다.

– 복호화

ASCII문자로 작성된 망령역이름설정화일을 조선어로 작성된 설정화일로 변환하는 지령입니다.

#kdnconv -r namedkp.conf1 > namedkp.conf2

-r: 역변환을 규정합니다.

namedkp.conf1: 변환하려는 화일이름

namedkp.conf2: 변환된 화일이름

· 문자렬복호화

#kdnconv -r

xn--o39a10a76y //변환하려는 ASCII문자렬을 입력합니다.

국가망 //결과가 출력됩니다.

5) 조선어망이름해결

사용자콤퓨터에 망령역이름봉사기의 주소(DNS Server주소)를 KDNS를 설치한 봉사기콤퓨터의 주소(실례로:172.16.200.83)로 설정합니다.

조선어망령역이름으로 홈페지를 호출합니다.

주의: 체계는 지정한 기본설정화일들을 정확히 리용하여야 합니다. 기본설정화일은 /etc/namedkp.conf 이며 구역화일들의 경로는 /var/named/masters 입니다.

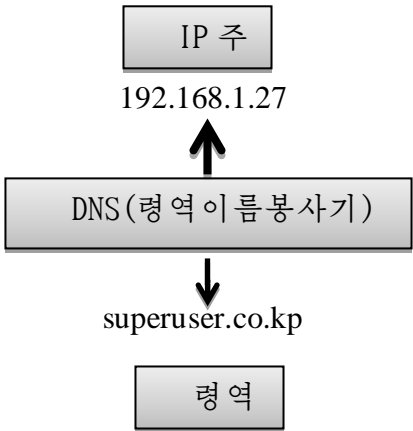
4. 일반망령역이름체계의 리용

1) 망령역이름봉사기에 대한 리해

령역과 IP 주소사이 관계

사람이 인터네트에 존재하는 수많은 봉사기들에 대하여 수자로 된 주소들을 모두 기억하기는 매우 불편하며 거의 불가능합니다. 그러므로 사람들은 수자로된 주소를 기억하기보다는 문자로 된 령역이름을 리용하게 되였습니다. 즉 IP 주소와 령역이름은 1:1 대응됩니다.

실례로 어떤 봉사기의 IP 주소가 192.168.1.27 이고 령역이름이 superuser.co.kp 라면 다음과 같이 령역이름봉사기를 통하여 1:1 대응되게 됩니다.

그림 19. 령역이름봉사

령역이름봉사기란 무엇인가?

IP 주소대신 령역을 리용하기위해서는 IP 주소와 령역을 각각 대응시키는 체계가 필요한데 바로 이러한 체계가 령역이름봉사기 (DNS)입니다.

령역이름봉사기의 우점에 대하여 보겠습니다.

DNS 가 나오기 이전에는 모든 사용자들이(리눅스를 사용하는) /etc/hosts 화일에 아래와 같은 형식으로 령역과 IP 주소의 대응을 직접등록하여 IP 주소와 령역을 인식하도록 하였습니다.

```
137.0.0.1        localhost.localdomain localhost
192.168.0.1      www
192.168.0.1      abc
192.168.0.1      def
```

이때에도 기본봉사기가 있었는데 이 기본봉사기가 하는 역할은 아주 단순하였습니다.

령역을 사용하기 위한 설정이 매번 불편하였으며 이런 난점을 극복하기 위한 과정에 령역이름봉사기(DNS)가 나오게 되였습니다.

IP 주소와 령역을 령역이름봉사기에만 등록해주고 각 말단들은 이 령역이름봉사기만 등록하여 이를 통해서 주소대응을 실현하였습니다.

2) 망령역이름봉사기의 설정과 리용

망령역이름봉사기의 설정

웨브봉사나 메일봉사를 받을 때 망령역이름봉사기를 리용하여 령역이름을 통해 이 봉사들을 제공받습니다.

망령역이름봉사기를 리용하려면 IP 주소와 령역을 대응시켜주며 그 봉사에 대한 설정을 진행하여야 합니다.

국부망에서 망령역이름봉사기능을 수행하기위한 설정을 실례를 통하여 설명합니다.

실례로 IP 가 192.168.1.7 인 콤퓨터에 example.co.kp 라는 령역이름을 대응시켜주고이 령역이름을 통한 웨브봉사기접속을 해봅시다.

우선 **/etc/namedkp.conf** 화일을 열고 다음과 같이 편집합니다.

```
<- 화일시작 ->
//
// namedkp.conf
//

options {
   listen-on port 53 {192.168.1.3; };  //여기에 현재 DNS 봉사기의 IP 주소를 줍니다.
   listen-on-v6 port 53 { ::1; };
   …
}

…

include “/etc/named.rfc1912.zones”;

//화일의 끝에 지역정보를 다음과 같이 편집합니다.

zone “example.co.kp” {  //령역이름을 “example.co.kp”로 합니다.
            type master;    //형은 master 로 줍니다.
            file “example.co.kp.db”;  //자료기지화일 이름을 줍니다.
};
<- 화일끝->
```

conf 화일을 편집하고 /var/named/masters 등록부안에 example.co.kp.db 라는 자료기지화일을 만듭니다.

/var/named/masters/example.co.kp.db 화일

```
$TTL 38400
example.co.kp.      IN      SOA     www. www.example.co.kp. (
                    1349355215
                    10800
                    3600
                    604800
                    38400 )
example.co.kp.      IN      NS      www.example.co.kp.
www.example.co.kp.          IN      A       192.168.1.7
```

이렇게 자료기지 화일을 만들어 준다음 령역이름봉사기를 재시동합니다.

방화벽설정

기정적으로 포구가 열려있지 않으므로 DNS 포구를 열어주어야 합니다.

포구설정은 다음과 같이 합니다.

지령 setup 으로 설정환경으로 들어갑니다. 여기서 [방화벽설정]을 선택하여 방화벽설정창문으로 넘어갑니다.다음 [사용자설정]단추를 눌러 다음 창문으로 가서 DNS 항목을 선택해주고 [완료]단추를 눌러 DNS 포구설정을 완료합니다.

망령역이름봉사기의 리용

망령역이름봉사기를 리용하여 의뢰기에서 봉사기호출을 IP 주소가 아니라 령역이름으로 할수 있습니다.

그러자면 의뢰기의 망설정에서 DNS 봉사기주소를 지정해주어야 합니다.

Windows xp 에서는 다음과 같이 설정합니다.

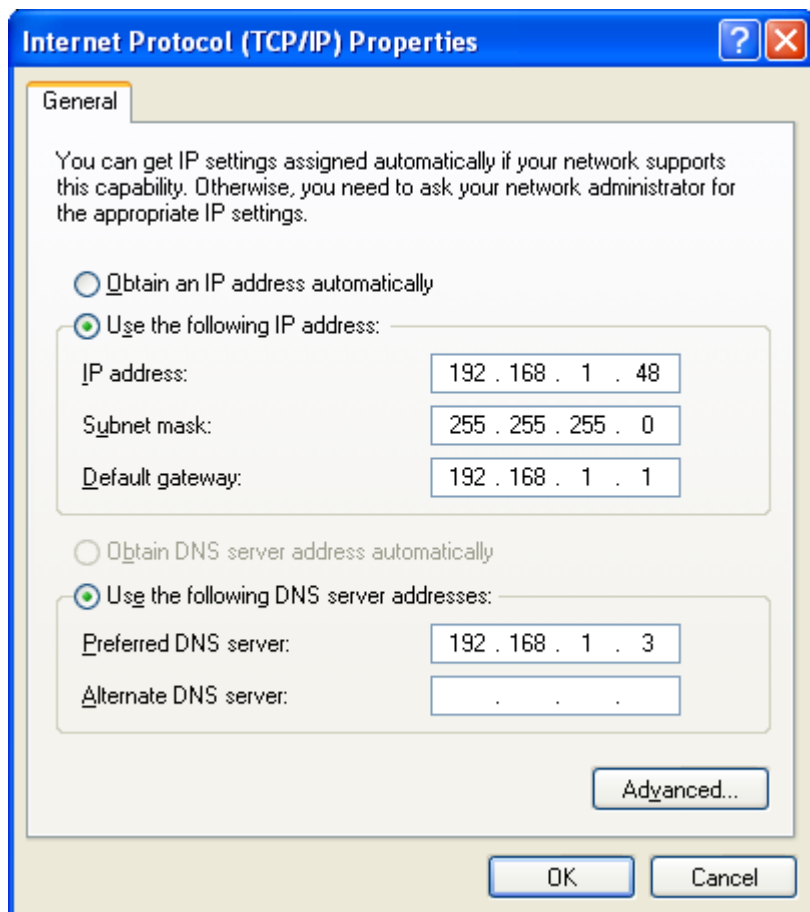



그림 20. Windows DNS 주소설정

≪붉은별≫사용자용체계 3.0 판에서는 체계환경설정을 기동하고 망을 선택합니다. 망설정창문에서 다음과 같이 설정합니다.

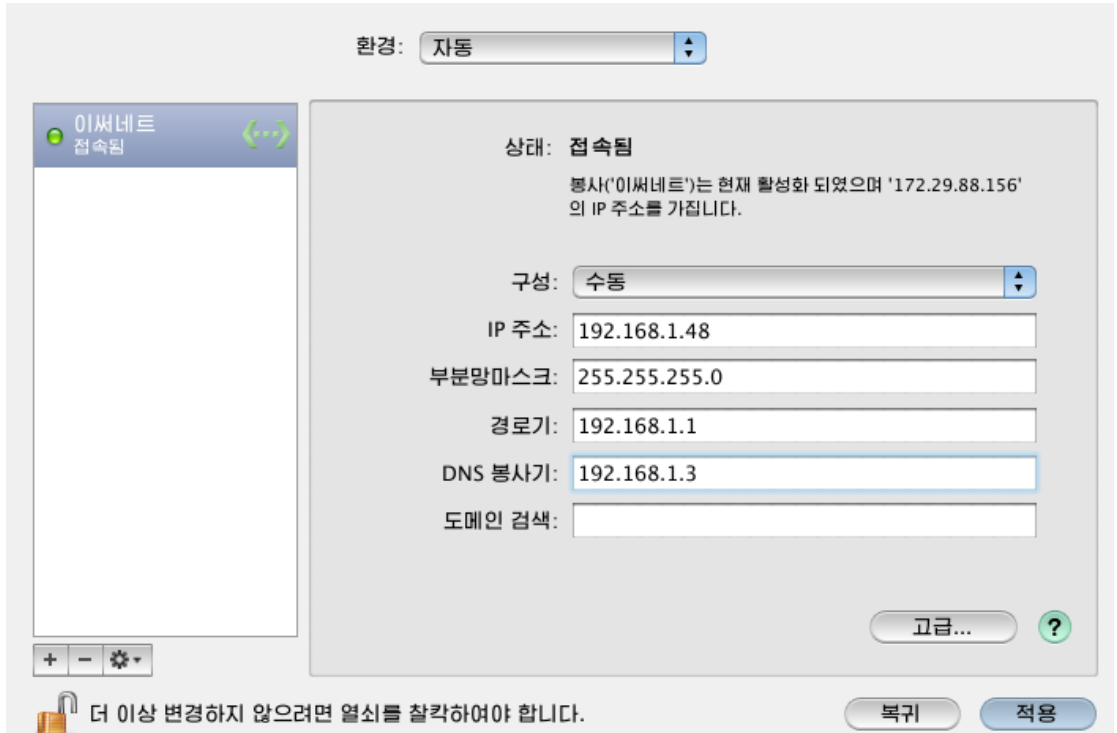



그림 21. DNS 주소설정

그러면 URL 주소를 령역이름으로 지정할수 있습니다.

제2절. 웨브응용쏘프트웨어봉사기

1. LAMP

1) 개요

LAMP(Linux, Apache, MySQL, PHP)는 《붉은별》 봉사기용체계 3.0에서 웨브봉사기인 Apache와 자료기지봉사기인 MySQL로 봉사기환경을 구축하고 웨브응용쏘프트웨어를 작성하여 기업경영활동의 정보화수준을 높이고 일반 사용자들로부터 제기되는 각종 웨브봉사를 진행하여주는 PHP에 의한 웨브응용쏘프트웨어개발환경입니다.

PHP는 http규약을 리용하여 자료기지관리체계인 MySQL봉사기에 방대한 자료를 저장 및 관리하여 사용자들에게서 제기되는 웨브봉사처리를 동적으로 진행하는 봉사기측실행스크립트언어입니다.

《붉은별》 봉사기용체계 3.0에서의 웨브응용쏘프트웨어개발을 위한 봉사기환경으로서 LAMP는 일반 사용자들의 웨브봉사를 위한 처리뿐만아니라 기업경영업무를 높은 정보화수준으로 올려세우는데서 중요한 자리를 차지합니다.

《붉은별》 봉사기용체계 3.0에서의 PHP의 판본은 5.3.2입니다.

배포판에는 php-5.3.2-6.rss3.0.i386.rpm으로 묶어져있습니다.

2) LAMP의 설치

LAMP를 설치하려면 우선《붉은별》 봉사기용체계 3.0을 설치할 때 모든 rpm들을 다 설치하여야 합니다. 즉 봉사기관련 실행rpm들을 모두 선택하고 설치하면 Apache 웨브봉사기나 자료기지봉사기(MySQL), PHP는 표준으로 설치되여있습니다.

· PHP의 설치확인

조작탁을 펼쳐놓고 다음의 지령으로 PHP의 설치를 확인합니다.

```
[root@localhost usr]#rpm –qa|grep php
php-5.3.2-6.rss3.0.i386.rpm
php-bcmath-5.3.2-6.rss3.0.i386.rpm
php-cli-5.3.2-6.rss3.0.i386.rpm
php-common-5.3.2-6.rss3.0.i386.rpm
php-dba-5.3.2-6.rss3.0.i386.rpm
php-debuginfo-5.3.2-6.rss3.0.i386.rpm
php-devel-5.3.2-6.rss3.0.i386.rpm
php-embedded-5.3.2-6.rss3.0.i386.rpm
php-enchant-5.3.2-6.rss3.0.i386.rpm
php-gd-5.3.2-6.rss3.0.i386.rpm
php-imap-5.3.2-6.rss3.0.i386.rpm
php-intl-5.3.2-6.rss3.0.i386.rpm
php-ldap-5.3.2-6.rss3.0.i386.rpm
php-mbstring-5.3.2-6.rss3.0.i386.rpm
php-mysql-5.3.2-6.rss3.0.i386.rpm
php-odbc-5.3.2-6.rss3.0.i386.rpm
php-pdo-5.3.2-6.rss3.0.i386.rpm
php-pgsql-5.3.2-6.rss3.0.i386.rpm
php-process-5.3.2-6.rss3.0.i386.rpm
php-pspell-5.3.2-6.rss3.0.i386.rpm
php-recode-5.3.2-6.rss3.0.i386.rpm
php-snmp-5.3.2-6.rss3.0.i386.rpm
```

```
php-soap-5.3.2-6.rss3.0.i386.rpm
php-xml-5.3.2-6.rss3.0.i386.rpm
php-xmlrpc-5.3.2-6.rss3.0.i386.rpm
php-tidy-5.3.2-6.rss3.0.i386.rpm
php-zts-5.3.2-6.rss3.0.i386.rpm
```

·Apache, MySQL의 시작방법

PHP는 봉사기용 스크립트언어이므로 웨브봉사기와 자료기지봉사기를 시작시켜야 합니다.

조작탁에서 다음의 지령을 실행하여 Apache, MySQL을 시작시킬수 있습니다.

먼저 Apache를 시작합니다.

```
[root@localhost usr]#service httpd start
httpd 봉사를 시작합니다 : [확인]
[root@localhost usr]#
```

다음으로 MySQL을 시작합니다.

```
[root@localhost usr]#service mysqld start
mysqld 봉사를 시작합니다 : [확인]
[root@localhost usr]#
```

봉사기대몬들을 중지 및 재시작하는 방법은 다음과 같습니다.

```
[root@localhost usr]#service httpd stop
httpd 봉사를 중지합니다 : [확인]
 [root@localhost usr]#service mysqld stop
mysqld 봉사를 중지합니다 : [확인]
[root@localhost usr]#service httpd restart
httpd 봉사를 중지합니다 : [확인]
httpd 봉사를 시작합니다 : [확인]
[root@localhost usr]#service mysqld restart
mysqld 봉사를 중지합니다 : [확인]
mysqld 봉사를 시작합니다 : [확인]
[root@localhost usr]#
```

3) LAMP의 사용방법

· 설정방법

PHP의 동작을 설정하기 위한 설정화일은 php.ini화일입니다. 이 화일은 PHP를 설치하면 기정으로 /etc에 위치됩니다.

여기서 몇가지 중요한 항목들을 설정하는것에 대하여 보기로 합시다.

```
engine = On;
```

```
asp_tags = Off;
display_errors = Off;
doc_root =”/var/www/html/”;
register_globals = Off;
extension=mysql.so;
extension_dir=”./”;
```

설명:

engine = On : Apache 상에서 PHP 스크립트언어엔진을 기동시키는 항목입니다.

asp_tags = Off : ASP 형식의 <% %>를 허용하는 항목입니다.

doc_root =”/var/www/html/”: 이 항목은 PHP 페지의 뿌리등록부를 설정해줍니다.

display_errors = Off : 이 항목은 스크립트의 실행과정에 일어난 오유들을 출력시키는 항목으로서 원격사용자들에게 로출되지 않도록 하여야 합니다. 이 항목을 능동상태로 놓는 경우에는 보안정보들을 로출시키므로 웨브봉사를 진행할 때에는 반드시 Off 로 설정하여야 합니다.

extension_dir = “/usr/lib/php/modules”: 적재가능한 확장자들이 있는 등록부들의 위치를 지정해주는 항목입니다. 기정으로 값이 정해져있지 않기때문에 우와 같이 설정하여 줍니다.

register_globals=Off : 이 항목을 피동상태로 놓으면 입력자료들에 대하여 대역변수들이 더이상 등록되지 않습니다. 사용자는 foo 변수대신에 $_REQUESR[“foo”]를 사용할수 있습니다.[“foo”]에는 request, namely, POST, GET 와 cookie 변수들을 통한 함수들이 선언될수 있습니다. 스크립트를 작성할 때 이 항목을 능동으로 놓는것을 피해야 합니다.

session.auto_start = 0 : 초기기동시 요청에서 쎄션을 초기화해주는 항목입니다.

upload_max_filesize = 2M : 화일을 올리적재할 때의 용량을 제한해주는 항목입니다. 기정값은 2Mbyte 입니다.

extension=mysql.so : 이것은 확장하려는 확장자이름을 설정해주는 항목입니다.

php.ini 화일은 일반적으로 php의 동작과 관련되는 여러가지 설정들을 진행할수 있는데 변경을 한 다음에는 꼭 httpd봉사를 재시작하여야 합니다.

```
[root@localhost usr]#service httpd restart
httpd 봉사를 중지합니다 : [확인]
httpd 봉사를 시작합니다 : [확인]
[root@localhost usr]#
```

· 동작검사

LAMP환경이 정확히 구축이 되여 PHP가 동작하는가를 확인하려면《내나라》열람기를 기동시켜 주소창에 http://localhost/를 입력하고 기동합니다.

이때 뿌리등록부에 있는 index.php화일이 실행되는가를 확인하여야 합니다.

구성화일 (php.ini)에 있는 뿌리등록부의 기정값은 /var/www/html입니다.

MySQL봉사기가 정확히 동작하는가를 보려면 조작탁에서 다음의 지령을 입력하여야 합니다.

```
[root@localhost usr]#mysql –u root –h localhost
MySql 조작탁의 리용을 환영합니다. 지령입력의 끝에 [;] 혹은 [\g]
를 붙여주십시오. 리용자의 MySql 접속식별자는 2 입니다.
봉사기판본:5.0.22
도움말을 보시면 <help>혹은 <\h>를 입력하십시오.
mysql>
```

> **주의:** PHP 를 리용하여 MySQL 과 련동하여 웨브페지를 작성할 때 조선말로 된 자료기지나 표를 창조하고 조선말자료를 입력 및 현시하는 경우 MySQL 봉사기와 접속한 다음 아래의 함수를 반드시 실행시켜야 합니다.
>
> mysql_query(set names utf8);

2. Apache 웨브봉사기

1) 개요

이 쏘프트웨어는 HTTP규약에 따라 망상에서 말단들에 html, cgi, php등에 의한 홈페지봉사를 해주는 웨브봉사기쏘프트웨어입니다

· HTML 봉사

사용자들은 웨브열람기(Internet Explorer 혹은 Naenara Browser)를 리용하여 웨브봉사기에 HTTP요청을 보낼수 있습니다.

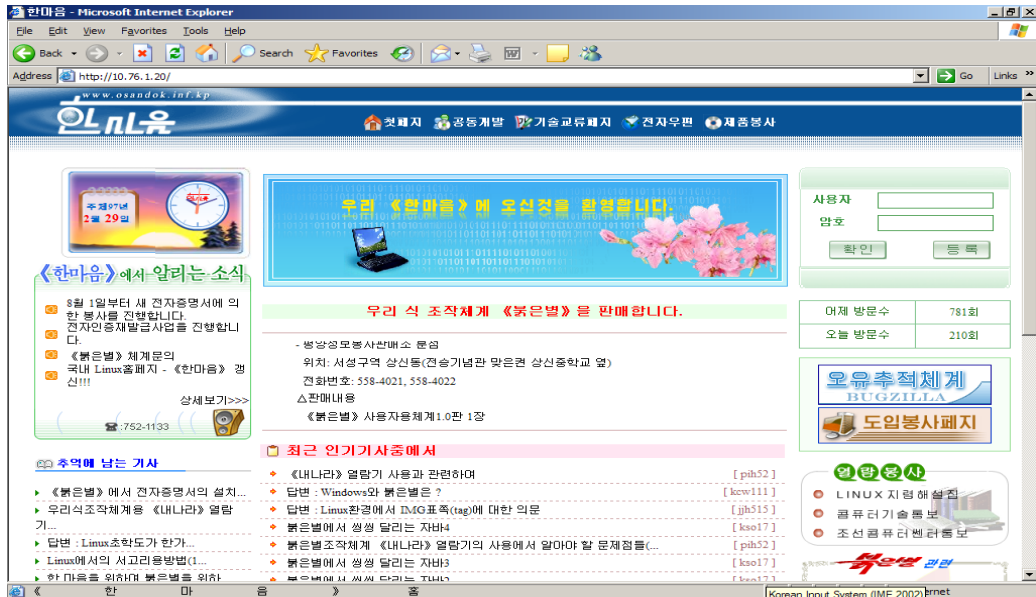



그림 22. 웨브봉사기에 의한 홈페지봉사

웨브열람기의 주소창(Address)에 우의 그림과 같이 http://10.76.1.20 이라고 쓰고 Enter건을 누르면 웨브봉사기가 해당한 내용을 열람기에 전송합니다.

HTTP규약에 따라 Html형식의 정보를 봉사해주는 봉사기를 웨브봉사기라고 합니다.

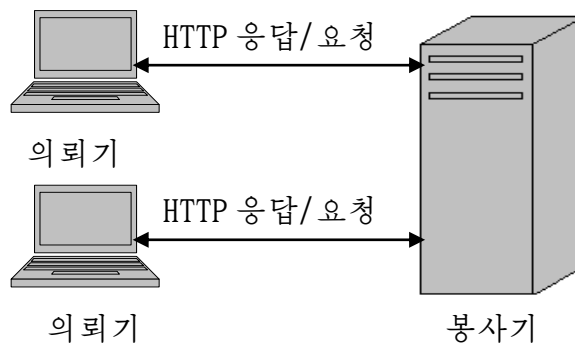



그림 23. 봉사기와 의뢰기사이의 HTTP 요청/응답

Apache웨브봉사기는 이러한 웨브봉사기들중에서 가장 리용률이 높은 봉사기입니다.

2) 설치와 해제

Apache웨브봉사기의 rpm이름은 httpd-2.2.15-5.rs3.0.noarch.rpm입니다.

Apache웨브봉사기는 《붉은별》 봉사기용체계 3.0이 설치될 때 자동적으로 설치됩니다.

체계가 설치된 후에《붉은별》 봉사기용체계 3.0의 제품CD나 그 복사본을 리용하여 httpd패키지와 관련패키지들을 수동적으로 설치할수 있습니다.

httpd패키지를 수동적으로 설치하는 경우에는 먼저 apr-1.3.3-4, apr-util-1.3.4-3 패키지가 설치되여있는가를 반드시 확인하여야 합니다. 이 패키지들이 없으면 httpd가 설치될수 없으며 강제적으로 설치하다고 해도 httpd 대몬이 정확히 실행될수 없습니다.

조작탁(konsole)에서 해당 패키지들이 설치되였는가를 확인합니다.

```
# rpm –qa | grep apr
```

이 지령을 입력하면 다음과 같은 결과가 현시되여야 합니다.

```
apr-1.3.3-4
apr-util-1.3.4-3
```

우와 같은 결과가 나오지 않으면 이 패키지들이 설치되지 않은것이므로 설치하여야 합니다.

CD를 리용하여 설치를 진행하는 경우에는 먼저 CD구동기에 《붉은별》 3.0(봉사기용체계)의 제품CD를 넣고 탑재를 시켜야 합니다.

```
# mount /dev/cdrom /mnt/cdrom
```

패키지들이 들어있는 등록부에서 설치하려는 패키지들이 있는가를 확인합니다.

먼저 apr, apr-util 패키지들을 설치합니다.

```
# rpm –ivh apr-1.3.3-4.rs3.0.i386.rpm
# rpm –ivh apr-util-1.3.4-3.rs3.0.i386.rpm
```

· 설치

httpd 와 httpd-manual 패키지를 설치합니다.

```
# rpm –ivh httpd-2.2.15-5.rs3.0.noarch.rpm
# rpm –ivh httpd-manual-2.2.15-5.rs3.0.noarch.rpm
```

참고: 만능표기문자(wildcard)《*》를 리용하여 여러개의 패키지를 한 번의 지령으로 설치하는 방법도 있습니다.

실례 : [root@localhost~]# rpm -ivh httpd* 이 지령을 사용하면 화일이름의 앞붙이가 httpd 로 되여있는 모든 패키지들이 다 설치됩니다.

· 해제

Apache 웨브봉사기를 삭제하려면 조작탁(konsole)에서 다음과 같은 지령을 실행시켜야 합니다.

#rpm –e httpd-manual
#rpm –e httpd

3) Apache 웨브봉사기의 리용

· 실행

rpm 으로 설치된 Apache웨브봉사기의 시작, 중지, 재시작과 같은 실행조종을 위해서 리용되는 지령에는 크게 3가지 부류가 있으며 부류별 리용에 따르는 결과는 같습니다.

[1부류] - 체계의 봉사기관리지령을 사용하는 경우

시작 : #service httpd start

중지 : #service httpd stop

재시작 : #service httpd restart

[2부류] - Apache웨브봉사기 고유의 실행화일이나 실행조종용 스크립트를 리용하는 경우

시작 : #httpd –k start

중지 : #httpd –k stop

재시작 : #httpd –k restart

[3부류] - 우의 경우에 httpd 대신에 apachectl을 사용해도 됩니다.

httpd 실행화일과 관련한 도움말 항목들은 –h 지령선택항을 리용하여 볼수 있습니다.

```
[root@localhost root]# httpd -h
사용법: httpd [-D 이름] [-d 등록부] [-f 파일]
              [-C "지시자"] [-c "지시자"]
              [-k start|restart|graceful|stop]
              [-v] [-V] [-h] [-l] [-L] [-t] [-S]
Options:
  -D 이름           : <IfDefine name> 지시자에서 사용하기 위한 이름을 정의 한다.
  -d 등록부         : 림시로 변경하여 사용하려는 ServerRoot의 경로를 지적합니다.
  -f 파일           : 림시로 변경하여 사용하려는 봉사기구성파일(ServerConfigFile
)의 이름을 지적합니다
  -C "지시자"       : 구성파일들(config files)을 읽기전에 처리하는 지시자
  -c "지시자"       : 구성파일들(config files)을 읽은후에 처리하는 지시자
  -e 수준값         : 수준값의 기동시 오유를 보여줍니다.(LogLevel 보기)
  -E 파일           : 기동시 오유를 기록하는 파일을 지정합니다.
  -v                : 판본정보를 보여줍니다.
  -V                : 콤파일 관련 설정내용을 보여줍니다.
  -h                : 가능한 명령행 항목들의 목록을 보여 줍니다. (이 페지에 준해
서)
  -l                : 콤파일되여 정적으로 련결된 모듈들을 보여줍니다.
  -L                : 구성가능한 지시자들(directives)의 목록을 보여줍니다.
  -t -D DUMP_VHOSTS : 현재의 가상호스트에 관해서만 분석된 내용을 보여줍니다.
  -S                : 우의 -t -D DUMP_VHOSTS 와 같은것 입니다.
  -t                : 구성파일(config file)의 문법이 맞는가를 검사합니다.
[root@localhost root]#
```

그림 24. httpd 의 열쇠단어들과 그에 대한 설명

우에서 언급된 세가지 방법중 [방법 2]를 사용하여 실제적으로 봉사기를 실행해 보는 경우 아래와 같이 된다면 봉사기가 정확히 실행된것입니다.

```
[root@localhost root]# /etc/init.d/httpd start
httpd봉사를 시작합니다:                                    [  확인  ]
```

우에 출력된것과 같은 통보문은 봉사기의 실행에는 지장을 주지 않습니다.

httpd가 정확히 실행되는가에 대해서는 아래와 같은 지령을 리용하여 알아볼수 있습니다.

[root@localhost root]# ps aux | grep httpd

이때 다음과 같은 결과가 현시되면 봉사기가 성과적으로 설치된것입니다.

이밖에도 내나라열람기를 기동시키고 주소띠에 http://localhost 라고 입력하였을 때 아래의 그림과 같은 화면이 현시된다면 Apache웨브봉사기가 성과적으로 설치된것입니다.

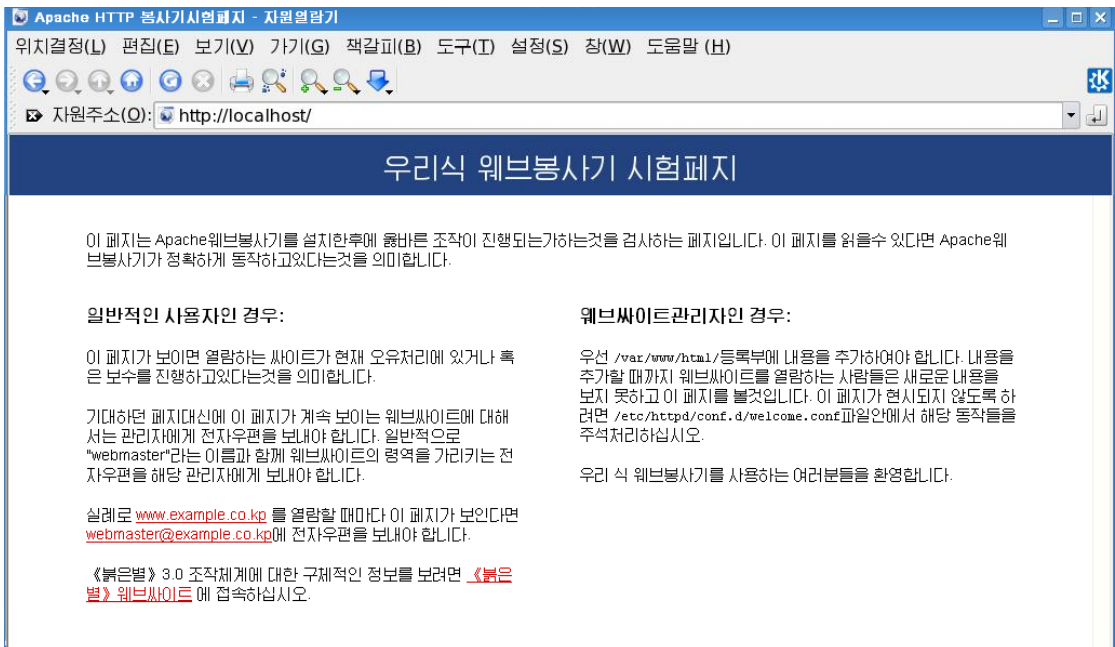



그림 25. Apache 웨브봉사기를 처음으로 설치했을 때의 호출화면

·httpd.conf을 리용한 웨브봉사기 간단한 설정

여기서는 Apache웨브봉사기 설정에 사용되는 httpd.conf 화일과 이것을 리용한 Apache봉사기의 설정과 관련한 가장 기본적이며 기초적인 설정에 대하여 설명합니다.

httpd.conf 화일을 변경한 다음에는 반드시 봉사기를 재시작하여야 합니다.

－ httpd.conf화일요약

앞에서 본것처럼 httpd.conf 화일을 Apache웨브봉사기의 동작을 위한 기본구성화일로서 여기에는 봉사기설정을 위한 각종 구성지시자들이 포함되여있으며 또 그외의 다른 지시자들을 추가할수 있습니다.

httpd.conf 화일은 크게 3개의 부분으로 되여있습니다.

첫번째 부분은 Apache웨브봉사기의 실행을 설정하기 위한 각종 지시자들로 이루어져있습니다.

두번째 부분은 주봉사기(main server)의 동작을 설정하기 위한 지시자들이 포함되여있습니다.

세번째 부분은 가상봉사기(Virtual server)설정 즉 하나의 콤퓨터상에서 두개이상의 웨브봉사기를 실행시키기 위해서 사용되는 지시자들이 포함되여있습니다.

각 부분들에서 설정된 매개 지시자들의 용도와 그의 설정내용은 httpd.conf 화일에 기본적으로 밝혀져 있습니다.

- 기본설정

Apache봉사기의 기본 봉사페지등록부는 /var/www/html 입니다.

때문에 작성된 홈페지로 웨브봉사를 하려면 표준적인 httpd.conf 화일의 내용을 조금 변경하여야 합니다.

httpd.conf 화일 변경과 관련하여 꼭 지켜야 할것은 이 화일을 변경한 후에는 꼭 Apache웨브봉사기를 재시작하여야 한다는것입니다.

이와 관련하여서는 우에서 설명하였으므로 더 취급하지 않습니다.

○ 기본봉사페지등록부의 변경

표준적인 httpd.conf 화일에는 기본봉사페지에 대한 설정이 DocumentRoot "/var/www/html" 로 되여있습니다.

만일 봉사하려는 홈페지가 “/var/www/html” 이 아닌 다른 등록부에 있다면 이것을 그 등록부경로로 바꾸어줍니다.

실례로 /usr/local/home 등록부에 있다면

DocumentRoot “/usr/local/home”

와 같이 설정하여야 합니다.

○ 기본봉사페지등록부에 대한 설정

기본봉사페지에 대한 설정을 변경시켰으면 그에 맞게 등록부설정도 변경시켜야 합니다.

즉 표준적으로

```
<Directory "/var/www/html">
        Options Indexes FollowSymLinks
        AllowOverride None
        Order allow,deny
        Allow from all
</Directory>
```

로 되여있다면 역시 “/var/www/html”을 변경시켜주면 됩니다.

우의 실례에서는 “/usr/local/home” 으로 바꾸어 줍니다.

○ 등록부 화일이름의 설정.

이 설정은 말단이 웨브봉사기의 등록부에 접근할 때 보여주기 위한 화일로서 표준적으로는

DirectoryIndex index.html index.html.var

로 설정되여있습니다.

여기에 사용자가 원하는 화일이름을 써주면 됩니다.

실례로 intro.html 이라는 화일로 설정하고 싶다면

DirectoryIndex index.html index.html.var intro.html

하고 추가적으로 밝혀주면 됩니다.

또한 index.html index.html.var를 제거하여도 됩니다.

우에서 보는바와 같이DirectoryIndex 지시자에는 여러개의 화일이름을 설정할 수 있으며 씌여진 순서가 우선권순서입니다.

때문에 사용자 intro.html을 추가적으로 밝혀주는 경우 등록부들에 index.html 이 있으면 이 화일이 먼저 말단에 보내지게 됩니다.

주의 : 이 사용지도서에서는《붉은별》 봉사기용체계 3.0 에 설치되여있는 httpd 를 실행하기 위한 가장 초보적인 내용만을 취급하므로 보다 구체적인 내용은 httpd- manual 패키지로 설치된 /var/www/manual 등록부의 설명서화일들을 참고하여 주십시오. 이 화일들에는 웨브봉사기운영에서 반드시 참고하여야 할 많은 정보들이 포함되여있습니다. 웨브봉사기가 실행되고있는 상태라면 《내나라》 열람기에서 http://localhost/manual/로 접근하여 이 설명서를 볼수 있습니다.

제3절. 자료기지봉사기(MySQL)

이 절에서는 자료기지봉사기(MySQL)의 구성과 기술적특성, 동작환경을 설명합니다.

1. 자료기지봉사기(MySQL)의 개요

1) 자료기지봉사기(MySQL)의 출현과 기술적특성

초기에 MySQL은 ISAM을 기본저장관리기로 하고 표조작은 mSQL을 리용하여 개발되였습니다. 그후에 속도와 유연성의 면에서 mSQL이 가지고있는 결함을 극복하기 위하여 새로운 관리체계를 만들게 되였으며 여기에 mSQL의 일부 API대면부들과 갱신된 API를 이식하는 방법으로 새로운 자료기지봉사기 MySQL이 출현하게 되였습니다.

MySQL은 가장 대중적이고 원천이 공개되여있으며 동시에 SQL자료기지봉사기입니다. MySQL은 다른 대형의 자료기지봉사기들에 비하여 속도가 훨씬 빠르고 사용하기 편리하며 개발자들이 쉽게 접근할수 있습니다. MySQL은 다중사용자, 다중쓰레드지원과 결합성, 속도, 안전성으로 하여 인터네트뿐 아니라 국내의 기관, 기업소들에서 대단히 많이 리용되고있습니다. MySQL은 또한 많은 응용쏘프트웨어들과 다국어환경을 지원하고있습니다.

MySQL의 중요한 특성들을 종합하면 다음과 같습니다.

- 핵심부쓰레드를 리용한 충분한 다중쓰레드를 제공하므로 다중 CPU를 사용할수 있습니다.
- C, C++, Eiffel, Java, Perl, PHP, Python, Tcl API들을 지원합니다.
- 각이한 조작체계환경들에서 작업할수 있습니다.
- 하나의 최량화된 다중결합을 리용한 매우 빠른 결합연산을 지원합니다.
- SQL함수들은 최량화된 클라스서고로 지원되며 실행속도가 빠릅니다.
- ANSI SQL, ODBC문법들과 마찬가지로 <LEFT OUTER JOIN>과 <RIGHT OUTER JOIN>을 지원합니다.
- 하나의 질문으로 각이한 자료기지의 표들을 혼합할수 있습니다.
- 매우 유연성있고 안전하며 주콤퓨터에 대한 신원검사를 허락하는 권한체계와 보안체계를 지원합니다. 접속할 때 모든 리용자정보는 암호화됩니다.
- 색인에 B나무를 리용합니다.
- 고정길이 및 가변길이기록들을 지원합니다.
- 대용량의 자료기지를 관리할수 있습니다. (현재 6만개의 표와 50억개의 행을 가진 MySQL을 리용하는 실례도 있습니다.)
- GNU 자동생성, 자동구성, 편리한 서고도구를 지원합니다.

- MySQL은 쓰레드에 기초한 기억할당체계를 리용하므로 기억소비가 적습니다.
- ISO-8859-1(Latin1), utf8, big5, ujis 등을 포함한 각이한 문자모임들을 지원합니다. 모든 자료는 선택된 문자모임으로 보관되며 표준적인 문자렬항목들의 비교에 영향이 없습니다. 그리고 모든 문자렬비교는 기본적으로 대소문자를 구별하지 않으며 현재의 문자모임에 의해 정렬순서가 결정됩니다. 정렬도 선택된 문자모임에 따라 진행됩니다. MySQL은 다국어로 말단에 오유통보문을 보낼수 있습니다.
- 말단들은 TCP/IP소케트나 Unix소케트(조작체계 UNIX에서)를 리용하여 MySQL봉사기에 접속할수 있습니다.
- MySQL 에서는 새로운 MyISAM저장관리기술을 적용하여 표크기를 최대8백만 TB까지 리용할수 있으며 표의 최대크기는 조작체계에 따르는 화일크기의 제한을 받습니다. (표 8. 참고)

표 8. 조작체계가 지원하는 표의 최대크기

조작체계	화일크기제한값
Linux-Intel 32 bit	4G 이상(Linux 판본에 의존)
Linux-Alpha	8T (Linux 판본에 의존)
Solaris 2.7 Intel	4G
Solaris 2.7 ULTRA-SPARC	8T (판본에 의존)

기정으로 자료기지봉사기(MySQL)의 표는 최대 4GB의 크기를 가집니다.

2) 자료기지봉사기(MySQL)의 구성

자료기지봉사기(MySQL)는 크게 의뢰기와 봉사기, 저장자료기지로 나누어볼수 있습니다.

자료기지봉사기(MySQL)의 일반적구조는 그림과 같습니다.

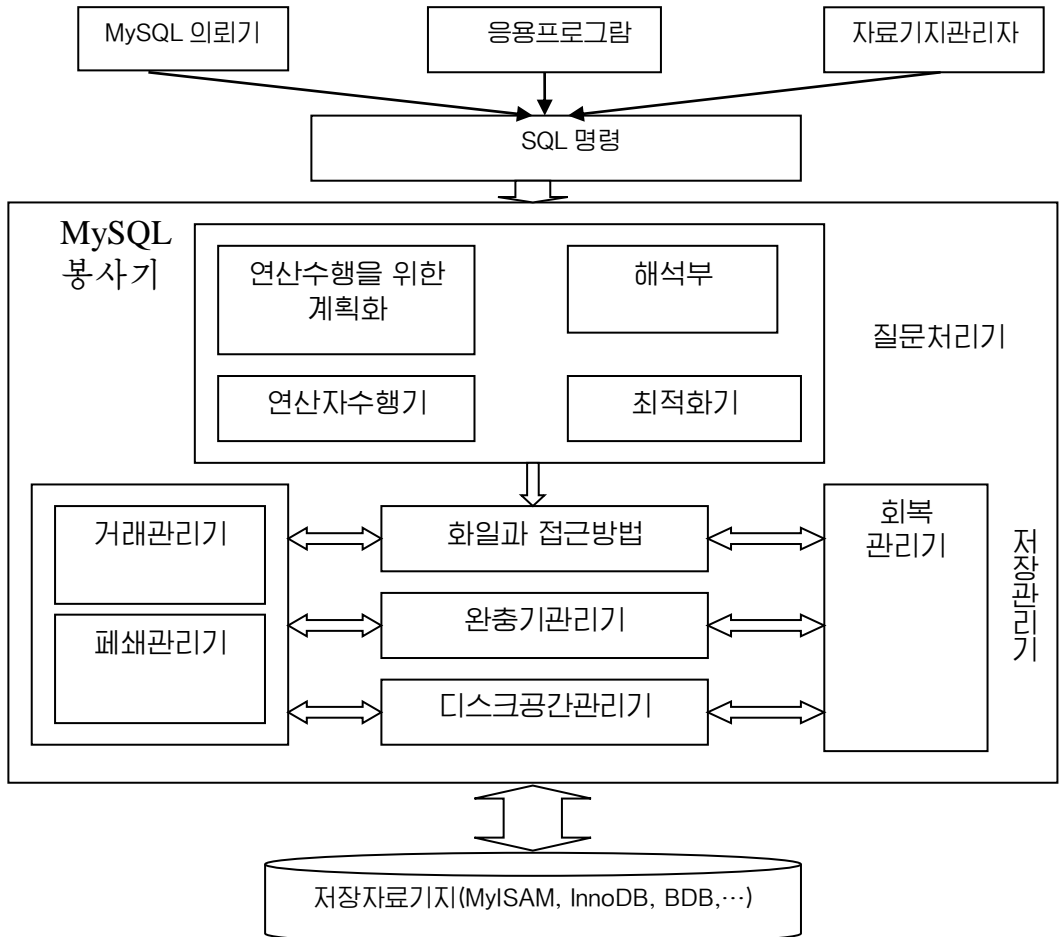



그림 26. 자료기지봉사기(MySQL)의 구성

의뢰기는 의뢰기전용쏘프트웨어를 리용한 사용자나 관리자 그리고 MySQL 자료기지를 리용하는 응용쏘프트웨어들입니다.

봉사기는 질문처리기와 저장관리기로 나누어 볼수 있습니다.

질문처리기는 사용자대면부로부터 입력된 SQL명령들의 해석을 진행하며 저장관리기는 디스크에 저장된 자료에 접근하고 관리하는 역할을 수행합니다.

자료기지봉사기(MySQL)는 다양한 사용자대면부를 통하여 SQL명령들을 받고 질문수행계획을 세우며 자료기지에 대하여 계획을 수행시킨 후 결과를 반환합니다. 사용자가 질문을 하나 만들어내면 이 질문은 질문 최적화기로 가며 여기서 자료저장에 관한 각종 정보를 참작하여 효률적인 수행계획을 수립합니다.

수행계획은 대체로 관계연산자의 나무로 표현되며 관계연산자들을 구현하는 코드들은 화일 및 접근방법계층우에 놓이게 됩니다. 화일 및 접근방법계층은 완충기관리기 계층우에 놓이며 이 계층은 디스크 읽기요청에 따라 이에 필요한 페지들을 디스크로부터 주기억장치로 가져옵니다.

자료기지봉사기의 제일 아래준위는 자료가 저장될 디스크공간을 관리하게 됩니다. 그우의 계층들은 디스크공간관리기라고 하는 계층이 제공하는 모듈들을 리용하여 페지의 할당, 반환, 읽기, 쓰기를 진행하게 됩니다.

자료기지봉사기는 사용자의 요청들을 분석하여 자료기지내의 각종 변경내용에 대한 리력를 유지함으로써 동시성과 장애복구를 지원합니다. 동시성조종 및 복구와 관련된 자료기지봉사기의 구성요소에는 다음과 같은것들이 있습니다.

거래관리기는 거래들이 적당한 페쇄규약에 따라 페쇄를 요청하거나 해제하도록 하고 그 수행을 관리합니다.

페쇄관리기는 자료개체에 대한 페쇄요청들을 감시하면서 가능해지면 페쇄를 하나씩 허가해줍니다.

복구관리기는 리력를 유지관리하며 체계에 손상이 생긴 후 체계를 다시 정상적인 상태로 복구하는 역할을 담당합니다.

디스크공간관리, 완충기관리, 화일 및 접근방법계층들은 긴밀히 호상작용하여야 합니다.

2. 자료기지봉사기(MySQL)의 설치와 삭제

1) 자료기지봉사기(MySQL)의 설치

봉사기패키지를 설치할 때 의존관계의 쏘프트웨어들이 있습니다. MySQL 5.5.18봉사기쏘프트웨어는 의존하는 패키지들이 설치된 조건에서만 설치됩니다.

필요한 패키지들은 체계가 표준적으로 제공합니다.

《붉은별》 봉사기용체계 3.0에서는 설치될 때 MySQL 자료기지봉사기를 같이 설치할수 있습니다.

체계가 설치된 후에 《붉은별》 봉사기용체계 3.0 제품CD나 그 복사본을 리용하여 MySQL패키지와 관련패키지들을 수동적으로 설치할수 있습니다.

CD를 리용하여 설치를 진행하는 경우에는 먼저 CD구동기에 《붉은별》 봉사기용체계 3.0 제품CD를 넣고 기동합니다.

패키지들이 들어있는 등록부에서 설치하려는 패키지들이 있는가를 확인합니다.

MySQL관련패키지들을 설치합니다.

설치순서는 다음과 같습니다.

- 우선 MySQL의뢰기패키지를 설치합니다.

```
[root@localhost mysql-5.5.18]# rpm -ivh MySQL-client-5.5.18-1.RSS3.i386.rpm
Preparing...                ########################################### [100%]
   1:MySQL-client           ########################################### [100%]
```

- 다음 MySQL봉사기패키지를 설치합니다.

```
[root@localhost mysql-5.5.18]# rpm -ivh MySQL-server-5.5.18-1.RSS3.i386.rpm
Preparing...                ########################################### [100%]
   1:MySQL-server           ########################################### [100%]
 조선어전문검색을 위한 조기화를 성과적으로 완료하였습니다.

 MySQL root 사용자의 통과암호를 설정하여야 합니다!
 그러자면 봉사기를 기동한 후 다음의 지령을 실행합니다:

 /usr/bin/mysqladmin -u root password 'new-password'
 /usr/bin/mysqladmin -u root -h localhost.localdomain password 'new-password'

 혹은 다음과 같이 할수도 있습니다:
 /usr/bin/mysql_secure_installation

 이것은 test자료기지를 삭제하는 선택항목을 주며 닉명의 사용자가
 표준적으로 창조되게 합니다.
 이것은 제품봉사기에 반드시 필요한것입니다.

 보다 상세한 정보는 사용지도서를 참고하십시오.
 [root@localhost mysql-5.5.18]#
```

봉사기패키지를 설치하면 자동적으로 초기자료기지가 구축됩니다.

2) 자료기지봉사기(MySQL)의 삭제

먼저 자료기지봉사기(MySQL)를 중지시킵니다.

다음 rpm -qa지령을 리용하여 현재 설치되여있는 MySQL 자료기지봉사기관련 패키지들의 이름을 얻습니다.

```
[root@localhost mysql-5.5.18]# rpm -qa | grep MySQL
MySQL-client-5.5.18-1.RSS3.i386
MySQL-server-5.5.18-1.RSS3.i386
[root@localhost mysql-5.5.18]# _
```

다음 rpm -e 지령으로 이 패키지들을 설치해제합니다.

```
[root@localhost mysql-5.5.18]# rpm -e MySQL-server
[root@localhost mysql-5.5.18]# rpm -e MySQL-client
[root@localhost mysql-5.5.18]#
```

3. 자료기지봉사기(MySQL)의 작업절차

1) 자료기지봉사기(MySQL)의 시작

패키지로 설치된 자료기지봉사기(MySQL)의 시작, 중지, 재시작과 같은 실행조종을 위해서 리용되는 질문에는 크게 2가지 부류가 있습니다.

부류별 리용에 따르는 결과는 같으며 어느 한 부류만 사용하여도 봉사기실행을 조종할수 있습니다.

- 시작 : #service mysqld start
- 중지 : #service mysqld stop
- 재시작 : #service mysqld restart

2) 자료기지봉사기(MySQL)의 접속

봉사기에 접속하기 위해서는 사용자이름과 통과암호를 주어야 합니다. 봉사기가 아닌 콤퓨터에서 접속한다면 주콤퓨터이름도 같이 주어야 합니다. 아래와 같이 봉사기에 련결할수 있습니다.

```
[root@localhost mysql-5.5.18]# mysql -uroot -hlocalhost
MySQL감시프로그람입니다.  지령끝은 ; 혹은 \g입니다.
MySQL접속식별자는 1입니다
봉사기판본: 5.5.18 MySQL Community Server (GPL)

Copyright (c) 2000, 2011.

도움말을 보려면 'help;' 혹은 '\h' 을 입력하십시오. 현재 입력한 명령을 지우려면 '\c'을 입력하십시오.

mysql>
```

<host>와 <user>는 MySQL봉사기가 돌아가고있는 주콤퓨터의 이름과 등록된 사용자이름입니다.

접속이 확립되면 일부 소개정보를 볼수 있으며 mysql>질문대기상태가 뒤따라 현시됩니다.

mysql>질문대기상태는 질문을 입력할수 있다는것을 의미합니다.

MySQL봉사기가 실행되고있는 콤퓨터에서 접속을 진행하는 경우 주콤퓨터이름을 생략합니다.

```
[root@localhost mysql-5.5.18]# mysql -uroot
MySQL감시프로그람입니다.  지령끝은 ; 혹은 \g입니다.
MySQL접속식별자는 1입니다
봉사기판본: 5.5.18 MySQL Community Server (GPL)

Copyright (c) 2000, 2011.

도움말을 보려면 'help;' 혹은 '\h' 을 입력하십시오. 현재 입력한 명령을 지우려면 '\c'을 입력하십시오.

mysql>
```

일부 MySQL설치판본은 봉사기주콤퓨터에서 리용자이름을 주지 않고 접속할수 있습니다.

이 경우 선택항목을 리용하지 않고 봉사기에 접속할수 있습니다.

```
[root@localhost mysql-5.5.18]# mysql
MySQL감시프로그람입니다.  지령끝은 ; 혹은 \g입니다.
MySQL접속식별자는 1입니다
봉사기판본: 5.5.18 MySQL Community Server (GPL)

Copyright (c) 2000, 2011.

도움말을 보려면 'help;' 혹은 '\h' 을 입력하십시오. 현재 입력한 명령을 지우려면 '\c'을 입력하십시오.

mysql>
```

봉사기와의 접속이 확립되면 언제든지 QUIT(또는 \q)를 mysql>질문대기상태에 입력하여 봉사기와의 접속을 완료할수 있습니다.

```
mysql> quit
안녕히 계십시오
[root@localhost mysql-5.5.18]#
```

3) 질문입력

Mysql의 일부 질문들을 실례를 들면서 질문입력의 기본원칙들을 서술합니다.

다음의 질문은 봉사기의 판본과 현재날자를 보여줍니다.

```
mysql> SELECT VERSION(), CURRENT_DATE;
+-----------+--------------+
| VERSION() | CURRENT_DATE |
+-----------+--------------+
| 5.5.18    | 2012-01-12   |
+-----------+--------------+
1 행이 있습니다 (0.00 초)

mysql>
```

우의 질문을 가지고 질문형식을 고찰해봅시다.

일반적으로 질문은 반두점으로 끝나는 SQL명령문으로 구성됩니다. (반두점이 생략되는 례외적인 경우도 있습니다. 앞에서 언급한 QUIT의 경우가 그 실례입니다.)

질문실행은 mysql의뢰기가 질문을 봉사기에 보내여 실행하도록 하며 그 결과를 화면에 현시하고 다음 질문대기상태를 보여주어 다른 질문에 대한 대기준비가 되였음을 알려줍니다.

Mysql의뢰기는 질문결과를 표형식(행과 렬)으로 보여줍니다. 첫행은 마당들의 이름이며 뒤의 행들은 질문결과값들입니다. 표준적으로 마당이름들은 실지 자료기지에서의 마당들의 이름입니다.

열쇠단어들은 대소문자를 구별하지 않습니다.

다음의 질문은 Mysql을 간단한 계산기로 사용하는 례를 보여줍니다.

```
mysql> SELECT SIN(PI()/4), (4+1)*5;
+--------------------+---------+
| SIN(PI()/4)        | (4+1)*5 |
+--------------------+---------+
| 0.7071067811865475 |      25 |
+--------------------+---------+
1 행이 있습니다 (0.00 초)

mysql> _
```

지금까지 질문들은 상대적으로 간단한 한행질문들이였습니다. 하나의 행에 여러개의 명령문 입력도 가능합니다. 각각의 명령문들은 반두점으로 구분합니다.

```
mysql> SELECT VERSION(); SELECT NOW();
+-----------+
| VERSION() |
+-----------+
| 5.5.18    |
+-----------+
1 행이 있습니다 (0.00 초)

+---------------------+
| NOW()               |
+---------------------+
| 2012-01-12 10:52:22 |
+---------------------+
1 행이 있습니다 (0.00 초)

mysql> _
```

mysql의뢰기는 명령문입력이 끝나는곳을 입력행의 끝으로 구분하는것이 아니라 반두점을 가지고 구분합니다. mysql의뢰기는 반두점이 나타나지 않으면 모든 입력행을 실행하지 않습니다.

다음은 간단한 여러행명령문을 보여줍니다.

례제에서 여러행질문의 첫행입력 후 질문대기상태가 ->로 변하는것을 보여줍니다.

```
mysql> SELECT
    -> USER()
    -> ,
    -> CURRENT_DATE;
+----------------+--------------+
| USER()         | CURRENT_DATE |
+----------------+--------------+
| root@localhost | 2012-01-12   |
+----------------+--------------+
1 행이 있습니다 (0.00 초)

mysql> _
```

질문입력과정에 입력한 질문을 취소하려는 경우 \c를 통해 질문을 취소할수 있습니다.

```
mysql> SELECT
    -> USER()
    -> \c
mysql>
```

질문을 다 입력하였지만 ->질문대기상태가 나타나면 반두점을 대기하는것입니다.

```
mysql> SELECT USER()
    -> ;
+----------------+
| USER()         |
+----------------+
| root@localhost |
+----------------+
1 행이 있습니다 (0.00 초)

mysql> _
```

'> 과 ">대기상태는 문자렬입력의 완료를 대기합니다.

```
mysql> SELECT * FROM 명단 WHERE 이름='김철송 AND 나이<30;
    '>
```

문자렬 입력취소도 \c를 리용합니다.

```
mysql> SELECT * FROM 명단 WHERE 이름='김철송 AND 나이<30;
    '> '\c
mysql>
```

4) 자료기지접근권한의 관리

봉사기에 존재하는 자료기지조사는 <SHOW>명령문을 사용합니다.

```
mysql> SHOW DATABASES;
+--------------------+
| Database           |
+--------------------+
| information_schema |
| 명단               |
| 비품관리자         |
| mysql              |
| performance_schema |
| test               |
+--------------------+
6 행이 있습니다 (0.01 초)

mysql> _
```

<mysql>자료기지는 사용자 접근권한을 관리하며 <test>자료기지는 시험용입니다.

<USE>는 <QUIT>와 마찬가지로 반두점을 요구하지 않습니다. (반두점으로 완료하는것도 가능합니다.) <USE>질문은 한행에서만 사용되여야 합니다.

례제에서와 같이 <test>자료기지를 사용할수 있지만 창조한 자료들은 다른 사용자에 의해 삭제될수 있습니다. 이 리유로 MySQL관리자에게 자기소유만의 자료기지를 사용할수 있는 권한을 요청해야 합니다. 자료기지 <비품관리자>를 호출하려고 하다고 가정하면 관리자는 다음과 같은 질문을 실행합니다.

```
mysql>
mysql> GRANT ALL ON 비품관리자.* TO 'root'@'localhost';
질문이 성공하였습니다. 0 행이 변경되였습니다 (0.01 초)

mysql>
```

<user>는 등록한 사용자이름이며 <host>는 봉사기에 접속하는 주콤퓨터의 이름입니다.

5) 자료기지의 창조및 관리

－ 자료기지의 창조 및 선택

자료기지의 창조는 <CREATE DATABASE>질문으로 합니다. 다음에 <비품관리자>라는 자료기지를 창조하는 실례를 보여줍니다.

```
mysql> CREATE DATABASE 비품관리자;
질문이 성공하였습니다. 1 행이 변경되였습니다 (0.00 초)
```

자료기지창조는 사용할 자료기지를 선택하지는 않으므로 반드시 리용을 위해서는 자료기지선택을 진행하여야 합니다. <비품관리자>를 현재 리용하려는 자료기지로 선택하기 위해서 다음의 질문을 사용합니다.

```
mysql> USE 비품관리자
자료기지가 변경되였습니다
mysql>
```

자료기지가 일단 창조되였다고 하더라도 사용하기 위해서는 <mysql>을 시작할 때마다 자료기지를 선택해야 합니다. 우의 례제와 같이 <USE>질문을 리용하는 방법이 있으며 mysql의뢰기를 호출할 때 자료기지를 직접 선택할수도 있습니다. 방법은 입력파라메터 다음에 자료기지의 이름을 입력하면 됩니다.

```
[root@localhost mysql-5.5.18]# mysql -uroot -p 비품관리자
Enter password:
MySQL감시프로그람입니다.  지령끝은 ; 혹은 \g입니다.
MySQL접속식별자는 4입니다
봉사기판본: 5.5.18 MySQL Community Server (GPL)

Copyright (c) 2000, 2011.

도움말을 보려면 'help;' 혹은 '\h' 을 입력하십시오. 현재 입력한 명령을 지우려면 '\c'을 입력하십시오.

mysql> _
```

질문에 있는 <비품관리자>는 사용자의 암호가 아닙니다. 질문의 -p선택항목 다음에 암호를 주려면 중간에 공백을 두지 말고 입력하여야 합니다. 암호를 질문 행에서 입력하는것은 봉사기에 가입한 다른 사용자에 의해 암호가 공개될수 있으므로 안전하지 못합니다.

– 자료기지속성의 변경

사용자는 <ALTER DATABASE>명령문을 리용하여 자료기지의 속성들을 변경할수 있습니다. 그 속성들은 자료기지 등록부의 <db.opt>화일에 저장되여있습니다. <ALTER DATABASE>를 사용하기 위해서는 사용자가 자료기지에서 ALTER 권한을 가져야 합니다. <ALTER DATABASE>라고 쓸수도 있고 <ALTER SCHEMA>라고 입력할수도 있습니다.

다음에 <비품관리자>자료기지의 문자모임속성을 <UTF8>로 변환하는 질문을 보여주었습니다.

```
mysql> ALTER DATABASE 비품관리자 CHARACTER SET UTF8;
질문이 성공하였습니다. 1 행이 변경되였습니다 (0.00 초)

mysql>
```

– 자료기지의 삭제

자료기지의 삭제는 <DROP DATABASE>명령을 리용하여 진행합니다. 다음에 <비품관리자>자료기지를 삭제하는 명령을 보여줍니다.

```
mysql>
mysql> DROP DATABASE 비품관리자;
질문이 성공하였습니다. 0 행이 변경되였습니다 (0.02 초)

mysql>
```

6) 표창조 및 속성변경

－ 표목록 보기

자료기지창조 후 자료기지안에는 표들이 존재하지 않습니다. 현재 자료기지에 있는 표들의 목록을 보려면 <SHOW TABLES>를 입력하면 됩니다.

```
mysql>
mysql> SHOW TABLES;
결과가 없습니다 (0.01 초)

mysql>
```

－ 표창조 및 속성보기

중요한것은 자료기지설계입니다. 즉 어떤 표가 필요하며 그 안에 각각 어떤 마당들을 넣어야 하는가에 대해 결정해야 합니다.

실례로 <비품목록>표를 다음과 같이 구성합니다.

표에 많은 다른 형태의 정보도 생각할수 있지만 다음과 같은것만으로도 충분합니다. (이름, 관리자, 특징, 종류, 접수날자 그리고 파손날자 등입니다.)

<CREATE TABLE>명령문을 사용하여 표의 설계를 진행합니다.

```
mysql> create table 비품목록( 이름 varchar(20),관리자 varchar(20),
    -> 특징 varchar(20),종류 varchar(20),접수날자 date,파손날자 date);
질문이 성공하였습니다. 0 행이 변경되였습니다 (0.04 초)

mysql> _
```

일단 표를 창조하면 <SHOW TABLES>는 다음과 같은 결과를 보여줍니다.

```
mysql> show tables;
+-----------------------------+
| Tables_in_비품관리자        |
+-----------------------------+
| 비품목록                    |
+-----------------------------+
1 행이 있습니다 (0.00 초)

mysql> _
```

어떤 표의 마당이름이나 마당들의 형태들에 대한 정보들을 얻으려면 <DESC> 또는 <DESCRIBE >질문을 수행합니다.

우의 례제에서 표가 제대로 창조되였는지 검사하기 위해 <DESCRIBE>명령문을 사용합니다.

```
mysql> describe 비품목록;
+--------------+-------------+------+-----+---------+-------+
| Field        | Type        | Null | Key | Default | Extra |
+--------------+-------------+------+-----+---------+-------+
| 이름         | varchar(20) | YES  |     | NULL    |       |
| 관리자       | varchar(20) | YES  |     | NULL    |       |
| 특징         | varchar(20) | YES  |     | NULL    |       |
| 종류         | varchar(20) | YES  |     | NULL    |       |
| 접수날자     | date        | YES  |     | NULL    |       |
| 파손날자     | date        | YES  |     | NULL    |       |
+--------------+-------------+------+-----+---------+-------+
6 행이 있습니다 (0.01 초)

mysql>
```

- 표의 이름 및 속성변경하기

<ALTER TABLE>을 리용하여 표의 구조를 변경할수 있습니다. 실례로 사용자는 마당의 추가와 삭제, 색인의 창조과 삭제, 현재 있는 마당의 자료형 그리고 표나 마당의 이름을 변경할수 있습니다. 표에서 마당들을 추가 혹은 변경할 때에는 <CREATE TABLE>과 비슷한 방법으로 합니다.

다음에 <비품목록>표에 <비고>라는 마당을 새로 추가하는 질문을 보여주었습니다.

```
mysql> alter table 비품목록 add column 비고 char(20);
질문이 성공하였습니다. 0 행이 변경되였습니다 (0.07 초)
Records: 0  Duplicates: 0  Warnings: 0

mysql>
```

표에서 <비고>마당을 삭제하려면 다음과 같이 입력합니다.

```
mysql> alter table 비품목록 drop column 비고;
질문이 성공하였습니다. 0 행이 변경되였습니다 (0.07 초)
Records: 0  Duplicates: 0  Warnings: 0

mysql>
```

<ALTER TABLE>명령으로 표의 이름을 변경할수도 있습니다. 다음에 <비품목록>표를 <비품>으로 이름을 변경하는 질문을 보여주었습니다.

```
mysql> alter table 비품목록 rename 비품;
질문이 성공하였습니다. 0 행이 변경되였습니다 (0.02 초)

mysql> _
```

<ALTER TABLE>명령을 리용하지 않고 <RENAME TABLE>명령으로 표의 이름을 변경할수도 있습니다.

아래에 <RENAME TABLE>명령을 리용하여 <비품>표를 <비품관리자>로 바꾸는 실례를 보여줍니다.

```
mysql> rename table 비품 to 비품관리자;
질문이 성공하였습니다. 0 행이 변경되였습니다 (0.06 초)

mysql>
```

– 표의 삭제

표의 삭제는 <DROP TABLE>명령으로 진행합니다. 다음에 <비품>표를 삭제하는 명령을 보여주었습니다.

```
mysql> drop table 비품목록;
질문이 성공하였습니다. 0 행이 변경되였습니다 (0.06 초)
mysql>
```

– 표에서의 자료조작

- 표에 자료입력하기

표를 창조한 다음에 표에 자료를 기입합니다. 표에 자료를 기입하는데는 <LOAD DATA>와 <INSERT>명령문이 리용됩니다.

<INSERT>명령문은 한번에 하나의 기록의 자료만을 표에 삽입하고 <LOAD DATA>명령문은 삽입하려는 자료를 본문화일에 써놓고 한번에 기입합니다.

실례로 행당 하나의 비품에 대한 기록을 가지고있고 매 값들은 태브로 구분되며 마당들이 순서로 되여있는 본문화일 <비품목록.txt>을 만들수 있습니다. 빈 값들은 <NULL>로 인식됩니다. 본문화일에서 <NULL>을 표현하기 위해서는 <\n>을 사용합니다.

본문화일 <비품목록.txt>를 <비품목록>표로 가져오기 위하여 다음의 질문을 사용합니다.

```
mysql> load data local infile '/var/lib/mysql/비품목록.txt' into table 비품목록;
질문이 성공하였습니다. 1 행이 변경되였습니다, 6 경고s (0.02 초)
Records: 1  Deleted: 0  Skipped: 0  Warnings: 6

mysql>
```

표에 하나씩 새로운 기록을 추가하는 경우 <INSERT>명령문을 리용합니다. 아래와 같이 <INSERT>명령문을 사용하여 기록을 추가할수 있습니다.

```
mysql> insert into 비품목록 values('책상2','한철국','밤색','사무용','1993/3/30',NULL);
질문이 성공하였습니다. 1 행이 변경되였습니다, 4 경고s (0.01 초)

mysql>
```

문자렬과 날자값은 인용부호를 사용하여야 하며 빈값을 나타내는 <NULL>을 직접 삽입할수 있습니다. <LOAD DATA>에서 사용한것과 같이 <\n>을 사용할수 없습니다.

실례로부터 간단한 <LOAD DATA>명령문을 사용하는 대신에 여러개의 <INSERT>명령문을 사용하여 초기자료들을 적재하는것이 많은 시간랑비라는것을 알수 있습니다.

- 표에서 자료변경하기

표에 이미 기입된 자료들을 변경하려는 경우 <UPDATE>명령을 리용하여 표에서 적당한 기록만 선택하여 수정할수 있습니다.

다음에 <비품목록>표에서 관리자이름이 <리창수>이던것을 <리창식>으로 변경하는 명령문을 보여주었습니다.

```
mysql> update 비품목록 set 관리자='리창식' where 관리자='리창수';
질문이 성공하였습니다. 0 행이 변경되였습니다 (0.00 초)
Rows matched: 0  Changed: 0  Warnings: 0

mysql> _
```

- 표에서 자료삭제하기

표에서 자료기록들의 삭제는 <DELETE FROM>명령으로 진행합니다. <DELETE>명령문은 표에서 모든 자료들을 한번에 지울수도 있고 지정하는 특정한 기록들만을 삭제할수 있습니다.

다음에 <비품목록>표에서 <관리자>마당값이 <리창수>인 항목을 삭제하는 명령을 보여줍니다.

```
mysql> delete from 비품목록 where 관리자='리창식';
질문이 성공하였습니다. 0 행이 변경되였습니다 (0.00 초)
Rows matched: 0  Changed: 0  Warnings: 0

mysql> _
```

- 표에서 자료검색하기
  - 한개 표에서 자료검색하기

<SELECT>명령문은 정보검색에 리용됩니다.

명령문의 일반적인 형식은 다음과 같습니다.

SELECT [선택마당목록] FROM [표이름] WHERE [조건];

가장 간단한 형태의 <SELECT>명령문은 표에서 모든것을 검색합니다.

```
mysql> select * from 비품목록;
+-----------+-----------+---------------+-----------+-------------+-------------+
| 이름      | 관리자    | 특징          | 종류      | 접수날자    | 파손날자    |
+-----------+-----------+---------------+-----------+-------------+-------------+
| 봉수산    | 리현성    | 소음 세다     | 선풍기    | 1999-09-12  | NULL        |
| 책상      | 한철국    | 밤색          | 책상      | 1993-04-02  | NULL        |
| 연상      | 김철송    | P3            | 콤퓨터    | 2000-07-03  | NULL        |
+-----------+-----------+---------------+-----------+-------------+-------------+
3 행이 있습니다 (0.00 초)

mysql>
```

전체표읽기는 간단합니다. <SELECT>명령문에서 <WHERE>구문을 생략하 됩니다.

표에서 특정한 행만 선택가능합니다. 실례로 <연산>콤퓨터의 파손날자를 확인하려면 아래와 같이 <연산>의 기록을 선택합니다.

```
mysql> select * from 비품목록 where 이름='연상';
+--------+----------+--------+----------+-------------+------------+
| 이름   | 관리자   | 특징   | 종류     | 접수날자    | 파손날자   |
+--------+----------+--------+----------+-------------+------------+
| 연상   | 김철송   | P3     | 콤퓨터   | 2000-07-03  | NULL       |
+--------+----------+--------+----------+-------------+------------+
1 행이 있습니다 (0.00 초)

mysql> _
```

표에서 반점으로 구분하여 주목하는 마당의 이름만 입력하면 됩니다. 비품접수 날자만을 검사하기 위해서 <이름>과 <접수날자>마당을 선택합니다.

관리자명단을 조사하기 위하여 아래의 질문를 사용합니다.

```
mysql> select 이름,접수날자 from 비품목록;
+------------+---------------+
| 이름       | 접수날자      |
+------------+---------------+
| 봉수산     | 1999-09-12    |
| 책상       | 1993-04-02    |
| 연상       | 2000-07-03    |
+------------+---------------+
3 행이 있습니다 (0.01 초)

mysql> _
```

<관리자>마당만을 검색하면 같은 이름이 여러번 반복됩니다. 이것을 피하기 위하여 <DISTINCT>를 리용합니다.

```
mysql> select distinct 관리자 from 비품목록;
+------------+
| 관리자     |
+------------+
| 리현성     |
| 한철국     |
| 김철송     |
+------------+
3 행이 있습니다 (0.02 초)

mysql>
```

<WHERE>구문을 사용하여 행선택과 렬선택을 서로 결합할수 있습니다.

```
mysql> select 이름,특징,접수날자 from 비품목록
    -> where 특징='P3' or 특징='선풍기';
+---------+---------+---------------+
| 이름    | 특징    | 접수날자      |
+---------+---------+---------------+
| 연상    | P3      | 2000-07-03    |
+---------+---------+---------------+
1 행이 있습니다 (0.00 초)

mysql> _
```

<NULL>값은 개념적으로 본다면 <루락된 알려지지 않은 값>을 의미하고 다른 값과는 조금 다르게 취급됩니다. <NULL>을 가지고 =, > 또는 <과 같은 산수비교연산자는 사용할수 없습니다.

```
mysql> select 1=NULL, 1<>NULL, 1<NULL, 1>NULL;
+--------+---------+--------+--------+
| 1=NULL | 1<>NULL | 1<NULL | 1>NULL |
+--------+---------+--------+--------+
|   NULL |    NULL |   NULL |   NULL |
+--------+---------+--------+--------+
1 행이 있습니다 (0.00 초)

mysql>
```

명백히 산수비교연산자를 가지고는 의미없는 결과를 얻습니다. <IS NULL>과 <IS NOT NULL>연산자를 사용합니다.

```
mysql> select 1 is NULL, 1 is NOT NULL;
+-----------+---------------+
| 1 is NULL | 1 is NOT NULL |
+-----------+---------------+
|         0 |             1 |
+-----------+---------------+
1 행이 있습니다 (0.00 초)

mysql>
```

MySQL에서 0 또는 NULL은 거짓(false)을 의미하며 다른것은 진실(true)을 의미합니다. 론리연산에서 진실은 1입니다.

두개의 NULL 값은 하나의 GROUP BY에서는 동등한것으로 됩니다.

<ORDER BY>를 실행할 때 <NULL>은 <ORDER BY ...ASC>를 하면 가장 먼저 나오고 <ORDER BY ...DESC>를 하면 가장 후에 나오는 값이 됩니다.

<NULL>을 리용할 때 범하는 일반적인 오유중의 하나는 <NOT NULL>로 정의된 칸에 0 또는 빈 문자렬을 삽입하는것은 불가능하게 생각하는것입니다. <NULL>이 <값을 가지고있지 않음>을 의미하는 반면에 이러한것들은 실지 어떤 값으로 존재합니다.

- 여러개의 표에서 자료검색하기

<SELECT>명령은 한개 표만이 아니라 여러개의 표들을 조합하여 자료검색을 진행함으로써 자료검색을 훨씬 쉽게 할수 있도록 해줍니다.

여러개의 표에서 정보를 검색하려면 <SELECT>명령문의 <FROM>다음 부분에 참조하려는 모든 표이름을 반점으로 구분하여 지정하면 됩니다.

여러개의 표에서 정보를 검색하는 <SELECT>명령문의 일반적인 형식은 다음과 같습니다.

SELECT [tb1.co1, tb2.co2] FROM tb1, tb2 WHERE [tb1.co1=tb2.co2];

여러개의 표에서 정보를 검색하는 <SELECT>명령문의 실례를 보여주기 위하여 <관리자명단>이라는 표가 다음과 같이 정의되였다고 봅니다.

```
mysql> select * from 관리자명단;
+---------+-----------+--------+
| 번호    | 이름      | 나이   |
+---------+-----------+--------+
|       1 | 리현성    |     23 |
|       1 | 김철송    |     23 |
+---------+-----------+--------+
2 행이 있습니다 (0.01 초)

mysql>
```

이제 나이가 23살인 관리자의 이름과 그가 관리하는 비품의 이름을 얻어내려고 할 때 <SELECT>명령은 다음과 같이 이루어집니다.

```
mysql> select 비품목록.이름,관리자명단.이름,관리자명단.나이 from
    -> 비품목록, 관리자명단 where
    -> 비품목록.관리자=관리자명단.이름 and
    -> 관리자명단.나이=23;
+----------+----------+-------+
| 이름     | 이름     | 나이  |
+----------+----------+-------+
| 봉수산   | 리현성   |    23 |
| 연상     | 김철송   |    23 |
+----------+----------+-------+
2 행이 있습니다 (0.00 초)

mysql> _
```

7) 조선어전문검색

조선어전문검색을 진행하기 위한 표의 창조는 다음과 같이 합니다.

```
mysql> create table 구호(번호 int,내용 text, fulltext(내용))engine=myisam;
질문이 성공하였습니다. 0 행이 변경되였습니다 (0.02 초)

mysql>
```

창조된 표에 자료들을 삽입하는 명령은 다음과 같습니다.

```
mysql> insert into 구호 values(9,"조국통일은 우리 인민의 세기적 숙망이다!");
질문이 성공하였습니다. 1 행이 변경되였습니다, 1 경고 (0.00 초)

mysql> insert into 구호 values(9,"세상에 부럼없어라!");
질문이 성공하였습니다. 1 행이 변경되였습니다, 1 경고 (0.00 초)

mysql> _
```

자료검색에서 조선어전문검색을 진행하는 명령은 다음과 같습니다.

```
mysql> select * from 구호 where match(내용) against("조국통일유훈");
+--------+----------------------------------------------------------------------+
| 번호   | 내용                                                                 |
+--------+----------------------------------------------------------------------+
|      9 | 위대한 수령님의 조국통일유훈을 철저히 관철하자                       |
+--------+----------------------------------------------------------------------+
1 행이 있습니다 (0.01 초)

mysql>
```

주의: 관리자는 매 사용자들에게 알맞는 접근권한을 부여해주어야 하며 특히 접근권한표들이 들어있는 <mysql>자료기지에는 관리자만이 접근할수 있도록 권한을 설정하여야 합니다. 관리자는 꼭 필요한 경우에만 <root>계산자리를 리용하고 일반적인 자료기지관리에서는 일반 사용자계산자리를 리용하여야 합니다. 만일 관리자가 <root>계산자리통과암호를 잊어먹는 경우가 있을수 있습니다. 이 경우에는 현재 가동중인 <MySQL> 봉사기를 끄고 다음과 같이 봉사기를 시작합니다.

[root@localhost usr]# mysqld --skip_ grant

통과암호를 설정한 다음에는 반드시 봉사기를 끄고 표준조작대로 봉사기를 다시 시작시켜야 합니다. 자료여벌복사를 정상적으로 진행하여야 합니다.

제4절. 우편봉사기(Postfix Server)

이 절에서는 우편봉사기(Postfix Server)를 설치하고 리용하는데서 우편봉사기의 절환방법과 봉사기의 봉사설정방법들을 설명합니다.

1. 우편봉사기 개요

우편봉사기(Postfix Server)는 망환경에서 말단들사이에 전자우편을 주고받을 수 있는 전자우편전송기능을 실현하게 하는 봉사기입니다. 우편봉사기(Postfix Server)를 리용하면 아주 쉽고 편리하게 우편봉사기를 구축할수 있습니다.

UNIX계렬의 조작체계들에서는 오래동안 Sendmail이 표준전자우편 전송봉사기로서의 지위를 차지하고있었습니다.

그러나 Sendmail은 설계사상이 낡은데다가 너무도 많이 수정되여 쏘프트웨어가 복잡하고 보안구멍(Security Hole)들이 많이 생겨났으며 설정화일을 서술하기가 매우 힘들다는 등 많은 문제점들을 안고있습니다. 그리하여 Sendmail을 대신하는 전자우편전송봉사기 쏘프트웨어로서 Postfix가 널리 쓰이게 되였습니다.

Postfix 우편봉사기(Postfix Server)는 Sendmail과 호환성이 높고 다른 전자우편봉사기로부터의 전환도 비교적 간단하기 때문에 많은 배포판들에서 표준으로 리용되고있습니다.

Postfix우편봉사기는 Sendmail과 비교하면 다음과 같은 우점을 가집니다.

- 설정이 쉽습니다 :

Sendmail의 설정화일인 sendmail.cf의 내용은 구조가 아주 복잡합니다. 그러므로 설정도구([CF]패키지나 sendmail에 부속되여있는 cf마크로)를 사용하여 sendmail.cf를 생성하는 식으로 설정을 진행하는것이 일반적이였습니다. 그래도 여전히 설정방법은 복잡하였고 또 Sendmail의 판본이 올라가도 설정도구가 갱신되지 않아 설정도구의 오유에 의한 설정실수도 자주 일어나군 하였습니다. 그러나 Postfix우편봉사기의 설정화일은 형식이 간단하여 알아보기 쉽고 전자우편전송의 동작과정도 리해하기 쉽게 서술되여있습니다.

- 처리속도가 빠르다 :

Sendmail은 기본적으로 전자우편을 한두통정도 처리하기 위한것이므로 다량의 전자우편을 목록화하여 전송하는 경우에는 smtpfeed 와 같은 배송대리자를 따로 정의하여야 합니다. 그러나 Postfix는 전자우편의 병렬전송기능을 가지고있으므로 다량의 전자우편도 비교적 짧은 시간동안에 송신할수 있습니다. 게다가 특정한 배송지에 갑자기 부하가 걸리지 않도록 동시배송수를 자체로 조종하는 [TCP slow start] 알고리듬을 실장하고있습니다.

- 안전성이 높다 :

Sendmail은 인터네트가 아주 평온할 때 만들어진 쏘프트웨어이므로 그 설계 자체에서부터 보안문제는 전혀 고려하지 않았습니다. 후날 보안상 문제가 제기되면 이구멍 저구멍 따라가며 메꾸는 식으로 퇴치하다보니 결과적으로는 쏘프트웨어가 비대해지고 유지하기조차 곤난해지게 되였습니다. 그러나 Postfix는 Sendmail의 이러한 문제점을 해소하기 위하여 개발되였고 보안상 충분히 고려하면서 설계된것입니다.

우편봉사기를 구축하고 우편봉사를 진행하자면 다음의 개념들에 대하여 알고 있어야 합니다.

SMTP(Simple Mail Transfer Protocol)

SMTP 는 전자우편을 전송하기위해 사용되는 TCP/IP 규약입니다.

사용하는 TCP 포구번호는 25 이며 상대측 봉사기를 지정하기위해 DNS 의 MX 레코드가 사용됩니다.

또한 전자우편봉사기사이의 우편송수신뿐만아니라 outlook 와 같은 의뢰기용 우편프로그람을 리용하여 우편봉사기로 우편을 보낼 때도 리용됩니다.

MTA(Mail Transfer Agent)

MTA 는 우편을 전문적으로 보내는 프로그람으로서 우편봉사기를 의미합니다. 사용자대리인으로부터 전자우편을 보내면 우편은 원천지의 MTA 로부터 목적지의 MTA 에 이르는 모든 MTA 들을 거쳐 전달됩니다. 현재 우리가 사용하는 Sendmail 이나 Postfix 가 기본 MTA 라고 볼수 있습니다.

MUA(Mail User Agent)

MUA 는 전자우편의뢰기프로그람을 의미합니다. 대표적인 프로그람으로서 outlook 나 《비둘기》(윈도우즈, 붉은별용), 《우편》(붉은별사용자용체계 3.0 판)을 들수 있습니다. 이 프로그람들은 사용자가 작성한 우편을 MUA 를 통하여 MTA 에 전달하고 자신의 수신함에 도착한 우편을 MTA 로부터 받아서 사용자에게 보여주는 역할을 수행합니다.

POP3(Post Office Protocol 3)

SMTP 가 우편을 전송하기 위한 규약이라면 POP3 은 MUA 와 MTA 사이의 련결을 조종하는 규약입니다. POP3 은 우편을 MTA 로부터 전송받은 다음 다시 MTA 에 접속하지 않고 수신된 우편을 관리할수 있게 합니다. 즉 POP3 은 보관하고 전달하는 봉사라고 할수 있습니다.

IMAP(Internet Message Access Protocol)

IMAP 는 POP3 과 마찬가지로 MUA 와 MTA 사이의 련결을 조종합니다. IMAP 는 POP3 에 비하여 봉사기에 등록부나 우편함을 만들어서 관리할수 있으며 우편을 삭제하거나 검색할수 있습니다. IMAP 는 POP3 과 같이 우편을 봉사기로부

터 전송받을수도 있지만 봉사기에 보관공간을 생성해놓고 자신의 기억기공간처럼 사용할수 있습니다.

2. 우편봉사기 설치

우편봉사기를 실현하는 기본설치패키지들은 다음과 같습니다.

- postfix-2.6.6-2.RSS3.i686.rpm
- dovecot-2.0-0.10.beta6.20100630.RSS3.i686.rpm
- dovecot-mysql-2.0-0.10.beta6.20100630.RSS3.i686.rpm

rpm지령을 리용하여 우의 패키지들을 설치합니다.

– 봉사의 시작

우편봉사기는 다음의 지령에 의하여 postfix대몬을 시작하여 시작합니다.

#service postfix start

– 봉사의 중지

우편봉사기는 다음의 지령에 의하여 중지시킵니다.

#service postfix stop

3. 우편봉사기 사용방법

1) 전자우편전송봉사기의 절환

Postfix가 설치되여있으면 체계가 리용하는 전자우편전송봉사기쏘프트웨어를 Sendmail로부터 Postfix로 절환합니다.

구체적으로는 관리자권한으로 alternatives지령을 실행하여 체계의 전자우편전송봉사기설정을 변경합니다.

alternatives --config mta

이렇게 하면 다음과 같은 안내가 표시됩니다.

```
2 개의 쏘프트웨어가 'mta'를 제공합니다.
  선택 명령
  -----------------------------------------------
  * +1 /usr/sbin/sendmail.postfix
     2 /usr/sbin/sendmail.sendmail

현재 선택[+]을 유지하려면 Enter건을 누르던가 아니면 선택번호를 입력하십시오:
```

Sendmail로부터 Postfix로 절환하기 위하여 [2][Enter]건반을 누릅니다. (설정을 변경하고 싶지 않을 때에는 아무것도 입력하지 않고 [Enter]만 누르면 됩니다.)

이제는 주콤퓨터가 재시작한 다음부터 Postfix가 자동적으로 시작하게 됩니다.

2) Postfix의 설정

Postfix의 기본적인 설정은 /etc/postfix/main.cf화일에서 진행합니다.

main.cf는 sendmail.cf와는 크게 차이나며 [파라메터 = 값]과 같은 단순한 서식으로 서술된 설정화일입니다.

대다수 설정은 기정으로 두고 최소한 설정하여야 할 항목들에 대해서 하나씩 설명합니다.

아래의 설정내용들은 망의 주소가 192.168.1.XXX 이고 부분망마스크가 255.255.255.0 이며 DNS 봉사기의 IP 주소가 192.168.1.24, 우편봉사기의 주소가 192.168.1.25 인 경우를 실례로 하였습니다.

- myhostname

myhostname 에서는 이 전자우편봉사기의 FQDN(Fully Qualified Domain Name)을 설정합니다. FQDN 은 다시 말하면 주콤퓨터의 완전한 이름, 즉 령역까지 밝힌 이름입니다. 행앞의 설명문기호[#]를 삭제하고 [주콤퓨터이름.령역이름]과 같은 형식으로 써넣습니다. 실례로 [mail.example.co.kp]라고 입력합니다.

myhostname = mail.example.co.kp

이 값은 example.co.kp 의 mail 봉사기라는것을 의미하게 됩니다.

- mydomain

[mydomain]에는 자기의 령역이름을 써넣습니다.

mydomain = example.co.kp

- myorigin

[myorigin]은 국부주콤퓨터에서 전자우편을 송신할 때 송신원주소에서 @다음에 추가하는 값을 설정합니다. 실례로 송신자의 주소를 person@domain.dom 으롤 lk 령역전체의 전자우편봉사기로 동작하도록 설정하는 경우에는 @mydomainm 을 지정합니다.

myorigin = $mydomain

우의 행은 결국 우편사용자의 식별자가 user1 이고 령역전체의 우편봉사기로 동작할 때 그의 주소가 user1@example.co.kp 로 된다는것을 의미합니다.

- inet_interfaces

여기에서는 전자우편을 수신하는 망대면부를 설정합니다. 기정적으로는 [localhost]가 선택되여 있지만 이 경우에는 원격으로부터 보내는 전자우편을 일체 수신할수 없습니다. 령역의 전자우편봉사기로 동작하게 하자면 원격으로부터의 전자우편전송도 접수하도록 [all]로 지정해주어야 합니다.

inet_interfaces = all

- mydestination

mydestination 은 도착한 전자우편이 자기한테 오는것인가 아닌가를 판단하기 위한 파라메터입니다. 령역의 전자우편전송봉사기인 경우 다음의 행을 유효로 하여 령역앞으로 오는 모든 전자우편을 이 전자우편전송사기가 수신하도록 하여야 합니다.

mydestination=$myhostname,localhost.$mydomain $mydomain

- local_recipient_maps

이 설정이 유효로 되여있는 경우 Postfix 는 국부사용자의 존재를 검사하여 불명확한 사용자앞으로 오는 전자우편의 수신을 거부합니다. 그러므로 유효로 해두는것이 좋습니다. 이것을 설정하면 Postfix 는 /etc/passwd 와 뒤에서 설명하는 alias_maps 의 설정에 따라 사용자에 대한 검사를 진행합니다.

local_recipient_maps= Unix:passwd.byname $alias_maps

- my_networks_styple 과 mynetworks

최근에 인터네트상에서 가장 중요한 문제의 하나가 스팜전자우편일것입니다.

여기서는 제 3 자중계를 방지하기 위한 설정을 진행합니다.

postfix 는 mynetworks_style 혹은 mynetworks 라고 하는 파라메터를 사용하여 신뢰할수 있는 SMTP 의뢰기를 판단합니다.

우의 실례와 같이 전자우편봉사기자신과 동일한 부분망으로부터 오는 전자 우편의 송신만 허가하는 경우에는 [mynetworks_style=subnet]와 같이 설정합니다.

mynetworks = 192.168.1.0/24

- home_mailbox

이 항목은 봉사기로 송신된 전자우편들을 보관하는 전자우편통의 보관방식을 지정합니다. Mailbox 또는 Maildir/라고 지정할수 있는데 Mailbox 라고 지정하는 경우에는 모든 전자우편자료를 ~/Mailbox 화일에 보관하여 관리하게 합니다. Maildir/라고 설정하는 경우에는 home/username/Maildir 등록부를 새로 생성하고 이 등록부를 리용하여 전자우편을 보관할수 있게 한다.

home_mailbox = Maildir/

2)Dovecot의 설정

Dovecot 의 기본적인 설정은 /etc/dovecot/dovecot.conf 화일에서 진행합니다. 이 화일을 편집기로 열어서 dovecot 를 구성합니다.

여기서 login_trusted_networks 파라메터설정부분을 찾아서 아래와 같이 수정합니다.

login_trusted_networks=192.168.1.0/24

이렇게 하면 전자우편봉사기를 리용하는 국부망은 192.168.1.0/21 로 제한합니다.

Dovecot 는 기정적으로 POP3 규약을 리용하여 우편을 전송합니다.

IMAP 나 다른 규약을 리용하는 경우에는 다음의 파라메터를 수정해야 합니다.

protocols = imap pop3 lmtp

기정적으로 이 파라메터는 [#]에 의하여 설정되지 않지만 imap 나 다른 규약을 리용하는 경우에 이 설명문기호를 없애야 합니다.

3) Postfix의 시작과 중지

Postfix 는 Sendmail 과 같이 TCP 의 25 번 포구를 청취합니다. 그러므로 사전에 Sendmail 이 기동하고 있을 때에는 이것을 중지하지 않으면 Postfix 가 기동할수 없습니다. 그러므로 먼저 Sendmail 이 기동하고 있는가를 확인하고 기동되여있다면 Sendmail 봉사를 중지시켜야 합니다.

다음의 지령을 리용하여 Sendmail 을 중지시킵니다.

service sendmail stop

Sendmail 이 중지되면 Postfix 를 기동합니다.

service postfix start

service dovecot start

우의 지령을 실행하면 Postfix 의 [master]데몬프로쎄스가 기동하고 있는데 master 는 주기억기에 상주하여 요구에 따라 Postfix 의 다른 모듈을 불러내는 역할을 하는 중요한 프로쎄스입니다.

우편봉사기의 중지는 stop 파라메터를 사용하여 진행합니다.

3) 우편의 전송

DNS 봉사기를 리용하지 않고 직접 우편을 전송하는 경우

우편봉사기설정부분에서 Postfix, dovecot 부분을 설정한다음 우편의뢰기프로그람에서 우편주소를 직접 IP 주소로 지정하여 우편을 전송할수도 있습니다.

이경우에는 우의 부분에서 DNS 봉사기설정부분이 필요없게 됩니다.

먼저 postfix 와 dovecot 를 우와 같이 편성한 다음 역시 우편사용자를 봉사기에 추가해줍니다.

다음 의뢰기프로그람을 리용하여 우편전송시험을 진행합니다.
이때 우편봉사기의 주소를 의뢰기프로그람에서 직접 입력합니다.
즉 의뢰기콤퓨터가 windows 체계인 경우 c:\windows\system32\drivers\etc\hosts 화일에서 우편봉사기퓨터 192.168.1.24 를 mail.example.co.kp 라고 지정해주고(물론 이이름은 postfix 의 myhostname 과 같아야 합니다) 의뢰기콤퓨터에서 봉사기주소를 maulu1@mail.example.co.kp 로 입력해주어야 합니다.
의뢰기콤퓨터가 붉은별조작체계인 경우에는 /etc/hosts 화일에 windows 에서와 같은 내용을 입력해주어야 합니다.
다음 IMAP/POP3, SMTP 봉사기의 주소도 역시 같은 방법으로 입력합니다.
이런 설정을 의뢰기프로그람에 적용하고 우편전송을 시험합니다.

DNS 봉사기를 리용하여 우편을 전송하는 경우

이 경우 DNS 봉사기가 이미 존재하고 이 봉사기에서 령역의 전자우편봉사기를 지정하며 이때 지정된 전자우편봉사기가 우편봉사기로 사용됩니다.
전자우편전송시험을 하기에 앞서 DNS(Domain Name Server)의 설정을 확인합니다.
이미 우에서 postfix 우편봉사기의 호스트이름을 mail.example.co.kp 로 설정하였습니다.
현재 DNS 령역이름을 example.co.kp 라고 할 때 그 봉사기에 mail.example.co.kp 를 등록해놓아야 합니다.
DNS 봉사기를 구성하기 위해 /etc/namedkp.conf 화일을 엽니다.
여기에 example.co.kp 라는 령역이름을 추가하여야 합니다.
먼저 Options 에서 현재 사용하는 DNS 봉사기의 IP 주소를 입력합니다.
listen-on port 53 { 192.168.1.25; };
다음으로 이 화일에 example.co.kp 라는 령역이름을 추가합니다.

```
zone "example.co.kp " {
   type master;
   file "example.co.kp.db";
   };
zone "1.168.192.in-addr.arpa" {
   type master;
   file "192.168.1.db";
   };
```

Db 화일을 편집해야 합니다.
Db 화일로서 /var/named/masters/192.168.1.db 와 example.co.kp.db 화일을 생성하고 구성해주어야 합니다.
192.168.1.db 화일:

```
$ttl 38400
1.168.192.in-addr.arpa.        IN      SOA     www.
www.example.co.kp (
                        1349355332
                        10800
                        3600
                        604800
                        38400 )
1.168.192.in-addr.arpa.        IN      NS      www.
24.1.168.192.in-addr.arpa.     IN      PTR
 www.example.co.kp
25.1.168.192.in-addr.arpa.     IN      PTR
 mail.example.co.kp
```

Example.co.kp.db 화일:

```
$ttl 38400
test.com.           IN      SOA     www. www.example.co.kp. (
                    1349355215
                    10800
                    3600
                    604800
                    38400 )
Example.co.kp IN    NS      www.example.co.kp
www.example.co.kp.  IN      A       192.168.1.24
mail.example.co.kp. IN      A       192.168.1.25
example.co.kp. IN   MX      10 mail.example.co.kp.
```

이와 같은 편성을 끝내고 DNS 봉사기를 시작합니다.

service named start

오유가 발생하는 경우에는 편성화일들이 잘못 편집되지 않았는가를 확인해보십시오.

다음으로 DNS 봉사기에서 우편봉사기의 호스트이름을 /etc/hosts 화일에 넣어줍니다.

192.168.1.25   mail.example.co.kp

DNS 봉사기가 성과적으로 기동하였을 때는 ping example.co.kp 와 ping mail.example.co.kp 지령을 리용하여 DNS 봉사기와 우편봉사기(mail.example.co.kp)가 기동하였는가를 확인해볼수 있습니다.

이때 주의할점은 의뢰기측 즉 우편을 보내려는 측에서 DNS 주소를 정확이 입력해주어야 한다는데 있습니다. 또한 현재 DNS 봉사기의 IP 주소가 192.168.1.24 라는데 주의를 돌리십시오.

DNS 주소는 setup 지령을 리용하여 [망설정]에서 설정할수 있습니다.

Postfix 봉사기가 가동하는 콤퓨터에서 DNS 주소를 192.168.1.24 로 입력하여야 합니다.

또한 우편송신자측에서 우편봉사프로그람의 pop3/imap 봉사기주소와 smtp 봉사기주소에 mail.example.co.kp 를 입력해야 한다는데 주의를 돌리십시오.

일반적으로 령역의 전자우편을 처리하는 봉사기는 DNS 의 정방향지역화일에서 MX(Mail Exchanger)레코드로 지정되여 있습니다. DNS 봉사기에 접근하여 다음과 같이 host 지령을 실행하면 DNS 의 MX 레코드에 관한 설정을 확인할수 있습니다.

host –t mx example.co.kp

DNS 봉사기에서는 우의 지령을 실행하면 현재 DB 화일에서 작성한것과 같이 example.co.kp 령역의 전자우편은 mail.example.co.kp.에 의하여 관리된다는 통보문이 현시됩니다.

DNS 의 설정이 정확하다고 확인되면 전자우편전송시험을 진행해봅니다.

시험을 진행하기전에 useradd 와 passwd 지령을 리용하여 우편사용자를 생성합니다.

useradd mailu1 –g mail

#passwd mailu1 지령을 실행하면 mailu1 사용자에 대한 암호를 입력합니다.

이 과정을 반복하여 여러명의 우편사용자를 생성한 다음 다음의 지령을 실행합니다.

service postfix restart
service dovecot restart

우의 지령을 리용하여 우편봉사기를 재기동시킵니다.

이때 /home/mailu1 등록부에 들어가보면 Maildir 라는 등록부가 생성되여 있는데 이 등록부에 이 사용자에게로 온 전자우편들이 보관되게 됩니다.

다음으로 의뢰기에서 outlook 나 비둘기를 리용하여 우편전송을 진행합니다.

이때 [전자우편주소]와 Pop3/imap, SMTP 봉사기의 주소를 정확히 입력하여야 합니다.

mailu1@example.co.kp
Pop3/Imap 주소 : mail.example.co.kp
SMTP 주소 : mail.example.co.kp

이렇게 가입을 진행한다음 mailu2 이나 mailu3 에로 우편을 전송하여 보면 봉사기가 정확히 동작하는가를 시험할수 있습니다.

4) 통합봉사기관리도구 ≪빛발≫을 리용한 우편봉사기의 구성

≪빛발≫에서 먼저 Postfix봉사기를 선택합니다.

다음으로 편성파일을 불러들이고 우에서 설명하였던 설정정보들을 입력해줍니다.

봉사기의 시작과 중지를 진행합니다.

이때 오유가 발생하면 편성파일편집에서 오유가 발생한것이므로 설정을 확인해보십시오.

다음으로 DNS봉사기를 구성합니다.

DNS봉사기를 선택하고 편성파일에 우에서 설명한 내용들을 추가합니다.

다음으로 우편봉사기를 MX레코드로서 추가해줍니다.

이름봉사기는 NS레코드로 추가합니다.

이름봉사기의 기동과 중지로 편성파일이 정확히 편집되였는가를 확인합니다.

편성에서 문제점이 발생하지 않은 경우 우편전송시험을 진행합니다.

5) 문제점 해결방법

만일 우편봉사기와 DNS 봉사기를 정확히 구성하였는데도 우편전송이 안되는 경우에는 방화벽설정에 대하여 확인하십시오.

방화벽설정은 setup 지령을 리용하여 진행합니다.

setup 지령을 입력하고 [방화벽설정]을 누르고 [사용자설정]단추를 누르면 여러가지 기존포구들에 대한 관리창문이 나옵니다. 여기서 SMTP 가 허락되였는가 허락되지 않았는가를 확인한 다음 만약 허락되지 않았을 경우에는 이것을 허락상태로 만들어주고 [완료]를 눌러서 끝냅니다.

만일 Postfix 에서 우편등록부를 기정경로(/home/username/Maildir)를 리용하지 않고 다른 등록부를 리용하는 경우에는 보안방책상문제가 제기될수 있으므로 이때는 보안방책을 다시 작성하여주어야 합니다.

제5절. 대리봉사기(Proxy Server)

1. 대리봉사기(Proxy Server) 개요

대리봉사기(Proxy Server)란 내부사용자에게 외부인터네트의 사용을 대리하는 봉사기를 의미하는것으로서 자료고속완충기능을 리용하여 내부사용자에게 빠른 인터네트속도를 제공하며 내부사용자의 자료보호를 위한 자체보안을 목적으로 하거나 또는 인터네트공유사용을 목적으로 하는 봉사기를 의미합니다.

대리봉사기를 사용하는 목적은 대부분이 고속완충봉사기로 리용하자는것입니다. 물론 경우에 따라서는 내부망의 보안을 위해서 사용하는 경우도 있습니다.

봉사기에서 대리봉사기로 사용할수 있는 패키지가 squid입니다.

Squid는 웨브의뢰기, FTP지원, 정보검색쏘프트웨어들 및 HTTP자료오브젝트 실현기능을 위한 고성능대리자고속완충봉사기입니다. 일반적인 고속완충쏘프트웨어와는 다르게 Squid는 단일방식 및 차단방식으로 입출력구동프로쎄스내에서의 모든 요구에 대한 조종을 진행합니다.

Squid는 메타자료를 관리하며 특히 RAM에서의 오브젝트고속완충기능, DNS조건탐색에 대한 고속완충기능, 차단방식의 DNS조건탐색지원기능을 지원하지만 실패한 요구에 대하여서는 고속완충을 리용하지 않도록 합니다.

Squid는 SSL, 확장접근조종, 그리고 모든 요구에 대한 가입을 지원합니다.

인터네트고속완충규약을 리용하여 Squid고속완충은 등급 또는 추가적인 대역폭부류를 재배렬합니다.

Squid는 요구 및 인증에 대한 재쓰기를 할수 있는 다른 선택적인 쏘프트웨어라고 말할수 있는 령역이름체계조건탐색쏘프트웨어인 기본봉사기 쏘프트웨어 squid와 일부 관리 및 의뢰기도구들로 구성되여있습니다.

> **참고** : 대리봉사기를 구축하여 직접 사용하려면 다음과 같은 점을고려하여야 합니다. 즉 대리봉사기는 많은 장점을 가지고있지만 내부사용자들의 의뢰기쏘프트웨어(웨브열람기등)에 대리봉사기사용을 위한 별도의 설정을 해야 하는 점이 결함이라고 할수 있습니다. 그리고 대리봉사기의 자료고속완충기능의 효률성이 현저하게 떨어질 경우에는 오히려 인터네트속도를 저하시키는 결함도 있습니다.

squid가 시작할 때 dns봉사기프로쎄스가 생성되고 단일방식으로 실행될 때와 차단방식으로 실행될 때의 DNS 조건탐색구성변수들이 생성됩니다. 이것은 DNS조건탐색을 위한 고속완충의 대기시간을 줄입니다.

2. 대리봉사기 설치

대리봉사기는 주봉사기쏘프트웨어인 Squid와 함께 령역이름봉사기검색 쏘프트웨어인 dnsserver 그리고 ftp자료를 가져오는 쏘프트웨어인 ftpget, 그리고 Squid관리도구와 의뢰기도구들로 구성되여있습니다.

대리봉사기를 실현하는 기본설치패키지는 다음과 같습니다.

squid-3.1.4-2.RSS3.i686.rpm

먼저 체계에 Squid가 설치되여있는가를 확인하려면 다음과 같은 지령을 실행시킵니다.

rpm –qa | grep squid

Squid가 설치되여있다면 해당한 판본정보까지 가진 패키지의 이름이 출력됩니다. 설치되여있지 않는 경우에는 아무런 결과도 나타나지 않습니다.

패키지를 설치하는 지령은 다음과 같습니다.

rpm –Uvh squid-3.1.4-2.RSS3.i686.rpm

대리봉사기쏘프트웨어를 설치하면 다음과 같은 화일 및 등록부들이 체계에 설치됩니다.

- /etc/squid : Squid의 기본등록부 - 이 등록부는 Squid의 기본설정등록부입니다. 이 등록부안에 기본 Squid설정화일인 squid.conf를 비롯한 여러가지 Squid설정화일들과 관련화일들이 존재합니다. squid.conf화일은 대리봉사기의 기본설정화일로서 대리봉사기의 주요한 기능과 역할을 결정하게 되는 아주 중요한 설정화일입니다. mime.conf화일에서는 대리봉사기에서 사용하는 MIME류형에 대한 설정을 진행합니다. msntauth.conf화일은 MSNT인증설정화일로서 대리봉사기에서 MSNT인증을 허용할 사용자와 허용하지 않을 사용자를 각각 설정하는 화일들에 대한 지시자가 설정되여있습니다.
- /usr/sbin/squid : Squid대몬화일 - 이 화일은 squid의 주대몬화일로서 정식이름은 대리고속완충기능봉사기입니다. /etc/rc.d/init.d/squid스크립트에 의해 시작/중지/재시작 될수 있습니다. 이 대몬이 실행되여있어야만 대리봉사기로 동작하게 됩니다.
- /usr/sbin/squidclient : Squid의뢰기쏘프트웨어 - 이 화일은 squid대리봉사기의 의뢰기쏘프트웨어입니다.

- /var/log/squid : Squid작업리력등록부 - 이 등록부는 대리봉사기의 리력화일이 저장되는 등록부입니다. Squid가 대리봉사기로 동작하게 되면 이 등록부에 리력화일을 저장하게 됩니다. 즉 대리봉사기로의 접근리력과 고속완충기능리력등이 저장됩니다.
- /var/spool/squid : Squid고속완충등록부 - 이 등록부는 Squid대리봉사기가 사용할 고속완충등록부입니다. 즉 고속완충된 자료가 저장되여있는 곳으로서 이 대리봉사기를 사용하는 사용자들에게 봉사될 고속완충자료가 존재합니다.

1) squid.conf의 파라메터들

대리봉사기의 기본구성설정화일은 /etc/squid/squid.conf화일입니다.

대리봉사기가 정상적으로 동작하도록 하려면 이 화일에서 다음과 같은 파라메터들을 설정하여야 합니다.

- http_port 3128 : 대리봉사기의 봉사포구번호는 3128입니다. 여기에서 대리봉사기가 리용하는 포구번호를 바꿀수 있습니다.
- cahce_mem 100MB : 대리봉사기에서 사용하는 고속완충기억기의 크기를 지정합니다. 기정으로 100MB로 설정되여있습니다.
- cache_dir ufs /var/spool/squid 100 16 256 : /var/spool/squid등록부를 고속완충등록부의 위치로 지정하고 고속완충등록부의 최대용량을 100MB로 지정하고 1차 부분등록부의 개수를 16개로 그리고 2차 부분등록부의 개수를 256개로 각각 지정합니다.
- cache_access_log /var/log/squid/access.log : 대리봉사기에 접근하여 접근한 의뢰기들의 리력를 기록하는 화일을 지정합니다.
- cache_log /var/log/squid/cache.log : 고속완충리력화일의 위치를 지정합니다.
- cache_store_log /var/log/squid/store.log : 고속완충관리의 활동상황을 기록하는 리력화일을 지정합니다. 즉 어떤 자료가 완충기에서 빠져나갔는지 또는 어떤 자료가 고속완충기에 저장되여 얼마나 오래동안 저장된 상태에 있었는가를 기록합니다.

- log_ip_on_direct on : 직접나가는 자료들에 대한 목적지 IP주소를 기록하게 합니다. 이전 판본에서는 IP주소대신 주콤퓨터이름을 기록하였습니다. 만일 이전 판본과 같이 주콤퓨터이름을 기록하려면 off값을 지정하면 됩니다.
- pid_filename /var/run/squid.pid : 대리봉사기대몬의 PID를 기록할 화일을 지정합니다. 만약 사용하지 않으려면 none을 입력합니다.
- cache_dns_program /usr/lib/squid/dnsserver : 대리봉사기가 사용할 DNS봉사기정보를 기록하고있는 화일을 지정합니다. 이 항목은 squid패키지의 번역시에 "--dissable-internal-dns"를 사용하여 설치하였을 때에만 유효합니다.
- dns_timeout 2 minutes : DNS질문시간으로 지정된 DNS봉사기들에 대한 질문을 할 때에 2분이상 질문에 대한 응답이 없다면 중단시킵니다.
- host_file /etc/hosts : 국부주콤퓨터이름봉사를 위한 주콤퓨터화일을 지정합니다. 즉 국부 DNS자료기지화일로 사용할 화일을 지정합니다. 대부분의 UNIX, LINUX조작체계에서 /etc/hosts화일을 국부 DNS자료기지화일로 사용하므로 그대로 설정해두면 됩니다.
- connect_timeout 1 minute : 이 항목은 TCP련결을 얼마나 오래 기다릴수있는가를 지정하는 값입니다. 기본값으로 1분으로 지정되여있으며 TCP련결에서 1분동안 아무러한 요청이 없는 경우에는 련결을 끝내게 됩니다.
- http_access deny all : 접근목록에 정의되여있는 설정들에 의존하여 대리봉사기에서 각 의뢰기들이 요청을 허용할것인가 아닌가를 결정하는 추간선택입니다. 이 화일에서는 아래실례와 같은 많은 접근목록을 정의하고있습니다.

```
acl Safe_ports port 80        #http
acl Safe_ports port 21        #ftp
acl Safe_ports port 443       #https
acl Safe_ports port 563       # snews

acl Safe_ports port 70        #gopher
```

acl Safe_ports port 210 #wais
acl Safe_ports port 1025-65536 #unregistered ports
acl Safe_ports port 280 #http-mgmt
acl Safe_ports port 488 #gss-http
acl Safe_ports port 591 #filemaker
acl Safe_ports port 777 #multiling http

- cache_mgr root : 국부고속완충관리자의 전자우편권한을 지정합니다. 즉 고속완충봉사기가 중지되였을 때에 받게될 전자우편권한(기정으로 root)을 설정합니다.
- cache_effective_user squid : 대리봉사기대몬을 어떤 사용자로 실행할것인가를 지정합니다. 보안을 위하여 다소 심중히 설계하여야 합니다. 만일 대리봉사기대몬을 실행할 때 root로 실행하였다면 이 설정과 같이 squid를 지정하도록 하십시오.
- cache_directory /usr/share/squid/icons : 그림기호화일들이 저장될 등록부를 지정합니다. 대부분 우에서와 같이 지정합니다.
- error_directory /etc/squid/errors : 대리봉사기에서 자료를 읽을 때에 오유가 생긴 화일들에 저장될 위치를 지정합니다. 기본 오유등록부는 /etc/squid/errors입니다.

2) squid 지령의 파라메터들

대리봉사기를 시작하게 하는 squid지령은 다음과 같은 여러가지 파라메터들을 리용하여 해당한 관리를 진행할수 있게 합니다.

-a : 들어오는 HTTP요구에 대한 바뀌는 포구번호를 지정합니다.

-d : 표준오유통보문에 대한 오유처리준위를 지정합니다. 이 항목을 리용하면 지정된 준위에서 오유처리통보문을 표준오유출구에 출력할수 있습니다.

-f : squid.conf화일의 위치를 지정합니다.

-h : 도움말정보를 출력합니다.

-k reconfigure : Squid가 구성화일을 다시 읽을 때 HUP신호를 전송합니다.

-k rotate : Squid가 리력화일을 회전시킬 때 USR1신호를 전송합니다. 알아둘것은 logfile_rotate가 0으로 설정되면 Squid는 모든 리력화일들에 대한 닫기 및 재열기를 진행합니다.

-k shutdown : Squid가 일시적으로 련결을 해제하고 끝낼 때 TERM신호를 보냅니다. 대기시간량은 shutdown_lifetime에서 지정할수 있습니다.
-k interrupt : 현재 련결에 대한 대기가 없이 직접적으로 Squid가 끝나는 경우 INT신호를 보냅니다.
-k kill : 모든 련결이나 리력화일들에 대해 관계 없이 Squid프로쎄스를 끝낼 때 KILL신호를 보냅니다.
-k debug : Squid가 다음 USR2신호를 받을 때까지 완전한 오유처리통보문을 만들려고 할 때 USR2신호를 보냅니다. 오유처리부분에서 유용합니다.
-k check : Squid프로쎄스에 “ZERO”신호를 보냅니다. 간단하게 프로쎄스가 실제로 실행되고있는가를 검사할수 있습니다.
-s : syslog에로 오유처리(오직 0준위)통보문을 전송합니다.
-u : ICP통보문에서의 변하는 포구번호를 지정합니다. 비표준포구에서의 구성화일검사에 유용합니다.
-v : Squid 판본을 출력합니다.
-z : 자기원판교환등록부를 만듭니다. 이 항목은 Squid를 처음 설치할 때 리용되며 또 cache_dir구성을 추가 및 변경하려고 할 때 리용합니다.
-D : 초기 DNS검사를 진행하지 않습니다. 대체로 Squid는 일부 공개되여있는 DNS주콤퓨터이름에 대하여서만 봉사를 제공하는 습관이 있습니다.
-F : Swap.state 리력이 없으면 고속완충기는 요구가 제기되기전에 “foreground”를 재구축합니다. 이것은 고속완충재구축시간을 줄이지만 HTTP 요구는 이 시간으로 만족되지는 않습니다.
-N : 자동적으로 배경대몬프로쎄스로 만들지 않습니다.
-R : 소케트에서 SO_REUSEADDR항목을 설정하지 않습니다.
-V : 가상주콤퓨터지원 Httpd-accelerator방식을 활성화합니다. 이것은 구성화일에서 httpd_accel_host 쓰기와 비슷합니다.
-X : 구성화일분석시의 완전한 오유처리기능을 활성화합니다.
-Y : swap.state화일을 읽을동안 ICP_OP_MISS 대신에 ICP_OP_MISS_NOFETCH를 되돌립니다. 만일 고속완충이 ICP를 리용한 자식고속완충기를 가지고있다면 보다 빨리 고속완충기를 재구축할수도 있습니다.

3. 대리봉사기의 작업절차

1) 구성화일squid.conf의 설정

대리봉사기를 정상적으로 기동하려면 다음과 같은 5가지 항목들을 새로 추가 설정하여야 합니다.

- 먼저 새로운 acl 규칙을 추가합니다.

  l mycenter src 172.29.88.0/21

  l mynet src 172.29.1.0/24

- 다음 새로 추가된 acl 에 대한 접근권한을 할당합니다.

  tp_access allow mycenter

  tp_access allow mynet

- squid 관리자의 우편주소를 설정합니다.

  cache_mgr root@test.com

- 고속완충등록부를 지정합니다.
  cache_dir ufs /var/spool/squid 100 16 256
- 고속완충기억기의 크기를 지정합니다.
  cache_mem 100 MB

앞에서와 같이 설정한 squid.conf화일의 내용은 아래와 같습니다.

```
#
# Recommended minimum configuration:
#
acl manager proto cache_object
acl localhost src 127.0.0.1/32
acl localhost src ::1/128
acl to_localhost dst 127.0.0.0/8 0.0.0.0/32
acl to_localhost dst ::1/128

# Example rule allowing access from your local networks.
# Adapt to list your (internal) IP networks from where browsing
# should be allowed
acl localnet src 10.0.0.0/8	# RFC1918 possible internal network
#acl localnet src 172.16.0.0/12	# RFC1918 possible internal network
#acl localnet2 src 192.168.0.0/16	# RFC1918 possible internal network
acl mycenter src 172.29.88.0/21	# hcb_add
acl mynet src 172.29.1.0/24	# hcb_add
acl localnet src fc00::/7 # RFC 4193 local private network range
acl localnet src fe80::/10 # RFC 4291 link-local (directly plugged) machines

acl SSL_ports port 443
```

```
acl SSL_ports port 631
acl SSL_ports port 15000
acl Safe_ports port 80          # http
acl Safe_ports port 21          # ftp
acl Safe_ports port 443         # https
acl Safe_ports port 631         # https
acl Safe_ports port 70          # gopher
acl Safe_ports port 210         # wais
acl Safe_ports port 1025-65535  # unregistered ports
acl Safe_ports port 280         # http-mgmt
acl Safe_ports port 488         # gss-http
acl Safe_ports port 591         # filemaker
acl Safe_ports port 777         # multiling http
acl CONNECT method CONNECT

#
# Recommended minimum Access Permission configuration:
#
# Only allow cachemgr access from localhost
http_access allow manager localhost
http_access deny manager

# Deny requests to certain unsafe ports
http_access deny !Safe_ports

# Deny CONNECT to other than secure SSL ports
http_access deny CONNECT !SSL_ports

# We strongly recommend the following be uncommented to protect innocent
# web applications running on the proxy server who think the only
# one who can access services on "localhost" is a local user
#http_access deny to_localhost

#
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS
#

# Example rule allowing access from your local networks.
# Adapt localnet in the ACL section to list your (internal) IP networks
# from where browsing should be allowed
http_access allow mycenter #hcb_add
http_access allow mynet #hcb_add
http_access allow localnet
http_access allow localhost

# And finally deny all other access to this proxy
#http_access deny all
```

```
# Squid normally listens to port 3128
http_port 3128

# We recommend you to use at least the following line.
hierarchy_stoplist cgi-bin ?

cache_mgr root@test.com          #hcb_add

# Uncomment and adjust the following to add a disk cache directory.
#cache_dir ufs /var/spool/squid 100 16 256
cache_dir ufs /var/spool/squid 100 16 256 #hcb_add

cache_mem 100 MB #hcb_add

# Leave coredumps in the first cache dir
coredump_dir /var/spool/squid

# Add any of your own refresh_pattern entries above these.
refresh_pattern ^ftp:                1440    20%     10080
refresh_pattern ^gopher:     1440    0%      1440
refresh_pattern -i (/cgi-bin/|\?) 0  0%      0
refresh_pattern .            0       20%     4320
```

2) 봉사의 시작과 중지

대리봉사기를 처음 설치하였을 때 먼저 교환구역등록부를 만들어야 합니다. 다음의 지령을 리용하여 교환구역을 생성합니다.

/usr/sbin/squid -z

교환구역이 생성된 후에는 다음의 지령에 의해서 대리봉사기를 실행시킬수 있습니다.

#service squid start.

또한 다음의 지령에 의하여 중지시킬수 있습니다.

#service squid stop

3) 대리봉사기의 동작확인

- 웨브봉사기설정

의뢰기에서 접속시험하려는 웨브봉사기를 설정합니다.

웨브봉사기는 대리봉사기쏘프트웨어를 설치한 봉사기에 설정하여 시험합니다.

웨브봉사기대몬은 httpd를 시작하고 여기에 접속하면 첫화면시험 폐지를 현시하여 시험해볼수 있으므로 다음의 지령을 리용하여 httpd대몬을 시작시키고 확인통보가 출력되는가를 확인합니다.

```
#service  httpd start
```

－ 의뢰기설정 및 대리봉사확인

먼저 웨브열람기에서 다음과 같은 방법으로 대리봉사기쏘프트웨어를 설치한 봉사기주소로의 웨브접속시험을 합니다.

http://172.29.88.225

앞에서 정확히 httpd대몬이 시작하였다면 의뢰기웨브열람기에서는 시험페지가 정확히 현시됩니다.

의뢰기에서 리용하는 웨브열람기쏘프트웨어에서 다음과 같은 순서로 대리봉사기설정을 진행합니다.

열람기의 도구차림표에서 인터네트추가선택->련결->국부망설정단추를 누릅니다.

국부망설정창문에서 대리봉사기사용검사단추를 그아래에 있는 고급선택단추를 누릅니다.

새로 펼쳐지는 대리봉사기설정창문에서 HTTP규약류형에 따르는 본문입력칸들에 대리봉사기의 주소와 포구를 입력하고 가운데부분에 있는 검사단추를 선택한 다음 〈확인〉단추를 누릅니다.

국부망설정창문에서 〈확인〉단추를 누르고 인터네트추가선택화면에서 〈확인〉단추를 누르면 대리봉사기설정이 끝납니다.

대리봉사기설정을 진행한 후에 다시 우에서 접속하였던 봉사기주소에로 웨브접속시험을 합니다.

열람기화면에 봉사기의 시험페지가 정확히 현시되는가를 확인합니다.

제6절. 동적주소할당봉사기(DHCP Server)

이 절에서는 《붉은별》 봉사기용체계 3.0에서 동적주소할당봉사기(DHCP Server)를 설치운영하기 위한 방법을 설명합니다.

1. DHCP 봉사기 개요

동적주소할당봉사기(DHCP Server)는 Dynamic host Configuration Protocol Server의 략자로서 동적인 IP할당을 위해 사용하는 규약이며 이를 실현한것이 dhcp봉사쏘프트웨어입니다. dhcp를 탑재하여 동적 IP주소할당봉사를 진행하는 봉사기를 dhcp봉사기라고 합니다.

dhcp봉사기는 구성화일과 관리대몬, 안내페지와 실행에 필요한 서고화일들로 구성되여있습니다.

동적주소할당봉사기(DHCP Server)가 비정상적으로 동작하는 경우 구성화일을 여벌복사한 상태에서 봉사패키지를 해제하고 다시 설치한 다음 여벌복사한 구성화일을 다시 해당한 위치에 복사하여 봉사를 재구성하여야 합니다.

2. 동적주소할당봉사기(DHCP Server)의 설치

dhcp-4.1.1-12.P1.RSS3.i686.rpm 패키지를 설치합니다.

rpm –ivh dhcp-4.1.1-12.P1.RSS3.i686.rpm

dhcp봉사기는 우리 식 조작체계《붉은별》 봉사기용체계 3.0이 설치될 때 자동적으로 설치됩니다.

동적주소할당봉사기(DHCP Server)패키지를 수동적으로 설치하는 경우에는 먼저 dhcp-4.1.1-12.P1.RSS3.i686.rpm패키지가 설치되여있는가를 확인하여야 합니다. 이 패키지들이 없으면 dhcp를 설치할수 없으며 강제적으로 설치한다고 해도 동적주소할당봉사기(DHCP Server)대몬이 정확히 실행될수 없습니다.

지령행에서 해당 패키지들이 설치되였는가를 확인합니다.

```
#rpm –qa | grep dhcpd
dhcpd-4.1.1-12.P1
```

우와 같은 결과가 나오지 않으면 이 패키지들이 설치되지 않은것이므로 설치하여야 합니다.

CD를 리용하여 설치를 진행하는 경우에는 먼저 CD구동기에 《붉은별》 봉사기용체계 3.0 CD를 넣고 탑재를 시켜야 합니다.

mount /dev/cdrom /mnt/cdrom

패키지들이 들어있는 등록부에서 설치하려는 패키지들이 있는가를 확인합니다. 확인이 끝나면 설치를 시작합니다.

3. 동적주소할당봉사기(DHCP Server)의 작업절차

1) 동적주소할당봉사기(DHCP Server)의 봉사시작과 중지

－ 봉사의 시작

조종탁에서 start지령을 주어 시작합니다.

#service dhcpd start 확인

－ 봉사의 중지

조종탁에서 stop지령을 주어 중지합니다.

#service dhcpd stop 확인

－ 봉사의 재시작

조종탁에서 restart지령을 주어 재시작합니다.

#service dhcpd restart 확인

2) 동적주소할당봉사기(DHCP Server)의 구성화일 설정

/etc/dhcp/dhcpd.conf는 dhcp봉사기의 기본구성화일입니다.

이 화일을 임의의 편집기로 열고 다음과 같이 입력합니다.

```
subnet 10.5.5.0 netmask 255.255.255.224 {
 range dynamic-bootp 10.254.239.40 10.254.239.60;
 option domain-name-servers ns1.internal.example.org;
 option domain-name "internal.example.org";
 option routers 10.254.239.1;
   option subnet-mask 255.255.255.0;
 default-lease-time 600;
 max-lease-time 7200;
}

host fantasia {
 hardware ethernet 08:00:07:26:c0:a5;
 fixed-address 10.254.239.43;
       }
}
```

항목들에 대한 설명은 다음과 같습니다.

① 먼저 subnet와 netmask항목에 국부망주소와 마스크를 지정합니다.
② routers항목에 의뢰기들이 사용할 관문주소를 설정합니다.
③ subnet-mask항목에 망마스크를 지정합니다.
④ domain-name-servers항목에 이름봉사기를 지정합니다.
⑤ domain-name항목에서 령역이름을 지정합니다.
⑥ range dynamic-bootp항목에서 의뢰기에 할당할 IP주소범위를 지정합니다.
⑦ default-lease-time항목에서 기정임대시간을 지정합니다. 지정단위는 초입니다.
⑧ max-lease-time항목에서 최대임대시간을 지정합니다. 지정단위는 초입니다.
⑨ 특정의 의뢰기에 고정된 IP주소를 할당하려는 경우
 - host항목에 콤퓨터이름을 지정합니다.
 - hardware ethernet항목에 MAC 주소를 지정를 지정합니다.
 - fixed-address항목에 할당하려는 IP 주소를 지정합니다.

dhcpd.conf 화일을 변경한 다음에는 반드시 봉사기를 재시작하여야 합니다.

제7절. 화일공유봉사기(Samba Server)

이 절에서는 화일공유봉사기(Samba Server)를 설치하고 리용하는데 필요한 사용방법들을 설명합니다.

1. 화일공유봉사기(Samba Server) 개요

Samba봉사는 의뢰기들에서 Unix체계봉사기의 화일들과 인쇄기들, 등록부들을 공유하여 리용할수 있도록 하는 봉사입니다.

많은 사람들이 Windows를 리용하는 자기의 의뢰기들을 여러 Unix봉사기들과 통합하여 리용하고싶어하였으며 Windows봉사기들과 Unix봉사기들을 통합하여 리용하는 경우에 의뢰기들을 관리하는데서 여러가지 문제점들이 제기되고 있었습니다. 또한 이전에 많이 리용하여 오던 망 화일관리규약들인 NFS, DecNet,

Novell NCP와 같은 규약들을 보다 리용하기 편리한 새로운 망화일관리규약으로 교체하고싶었습니다. 이러한 요구로부터 출발하여 개발된 망화일관리규약이 바로 Samba봉사규약입니다.

Samba가 포함하고있는 간단한 기능목록들을 아래에서 개괄하여 설명합니다.

- Samba봉사기는 Windows NT, LAN Manager-style 화일 및 인쇄봉사들을 Windows 95, Warp Server, smbfs 등과 같은 Samba의뢰기들에 제공합니다.
- Windows NT 4.0 령역조종기(Domain Controller)를 대신합니다.
- Windows NT 4.0의 성원으로서 또는 Active Directory domain으로서 동작할수 있는 화일및 인쇄봉사기입니다.
- NetBIOS (rfc1001/1002) 이름봉사기로 리용할수 있습니다. Samba는 필요한 경우에 국부망에서 기본열람기로 리용될수 있습니다.
- Samba 의뢰기들은 Unix와 같은 다른 조작체계들로부터 자기원판이나 인쇄기들과 같은 개별콤퓨터자원들에 접근할수 있습니다.
- 개별콤퓨터들의 여벌복사를 위해서 tar확장자를 지원합니다.
- 일부 NT관리기능들을 지원하는 제한된 지령행도구를 제공합니다.

Samba는 화일들과 인쇄기들을 공유하고 또 화일들이나 등록부들에 대한 목록과 같은 다른 정보들을 공유하게 하는 규약입니다. 이 규약을 이미 지원하고 있는 조작체계들은 Windows 9x, Windows NT계렬, OS/2, Mac OS X, Linux등입니다. 일부 웨브열람기들에서도 이 규약을 리용할수 있도록 《smb://》를 지원하고있습니다. Samba를 리용하면 아주 쉽고 편리하게 화일봉사기를 구축할수 있습니다. Samba는 특별한 의뢰기쏘프트웨어를 리용하지 않아도 우리가 가장 흔하게 사용하는 웨브열람기나 화일열람기를 리용하여 아주 편리하고 쉽게 화일을 내리적재 및 올리적재할수 있습니다. 또한 간단하게 망구동기를 설정하기만하면 원격지의 Samba봉사기에 있는 특정한 등록부를 자기의 열람기내부의 구동기로 사용할수도 있습니다. 즉 원격지봉사기의 특정등록부를 자신의 콤퓨터에 있는 하나의 하드구동기처럼 사용할수 있습니다.

원래 Samba는 다른 종류의 조작체계들에서 자원을 공유하기 위한 목적으로 개발된 응용쏘프트웨어입니다. 즉 망인쇄기를 설정하여 인쇄기공유를 하던가 망을 리용한 자원공유를 위한 목적으로 사용할수 있습니다. Samba에는 이와 같

은 여러가지 기능들이 있지만 잘 사용하지 않는 기능과 불필요한 기능도 있으며 여기에서는 현재 가장 많이 리용되는 기능인 망화일체계의 공유방법에 대한 설명을 위주로 하여 설명합니다.

2. 화일공유봉사기(Samba Server) 설치

Samba봉사기를 실현하는 기본설치패키지들은 다음과 같습니다.

- samba-3.5.4-68.RSS3.i686.rpm
- samba-client-3.5.4-68.RSS3.i686.rpm
- samba-common-3.5.4-68.RSS3.i686.rpm
- samba-winbind-clients-3.5.4-68.RSS3.i686.rpm

rpm지령을 리용하여 우의 패키지들을 설치합니다.

설치한 Samba패키지들에 의해 생성된 중요한 Samba관련화일들의 이름과 그 화일들의 역할을 아래에 설명합니다.

- /etc/logrotate.d/samba : Samba작업기록을 관리하기 위한 스크립트화일입니다.
- /etc/rc.d/init.d/smb : Samba봉사기의 대몬(smb, nmbd)을 실행(끝내기,재시작)하기 위한 스크립트화일입니다.
- /usr/bin/smbstatus : Samba봉사기에 사용자가입한 정보를 확인하기 위한 편의프로그람입니다.
- /usr/sbin/nmbd : smb NetBIOS대몬
- /usr/sbin/smb :Windows봉사기와 화일 및 인쇄기공유를 위한 Samba봉사기의 기본대몬입니다.
- /usr/bin/smbclient : smb의뢰기편의프로그람로서 smb봉사기에로 접속하게하는 기능을 제공합니다.
- /etc/samba/ : Samba봉사기설정과 관련한 기본등록부입니다.
- /etc/samba/lmhosts: Samba봉사기 NetBIOS주콤퓨터화일 (smb봉사기에서 사용하는 주콤퓨터정보화일)입니다.
- /etc/samba/smb.conf : Samba봉사기의 기본설정화일입니다.
- /usr/bin/testparm : Samba봉사기설정화일(smb.conf)을 검사해보는 편의프로그람입니다.
- /var/log/samba/ : smb리력정보가 저장되는 등록부입니다.

- /etc/samba/smbusers : 체계사용자식별자와 Samba사용자식별자가 다른 경우에 이를 정합시키기 위한 정합표화일입니다.

3. 화일공유봉사기(Samba Server)의 작업절차

1) 봉사의 시작과 중지

－ 봉사의 시작

Samba봉사기는 다음의 지령에 의하여 smb대몬을 시작하여 시작합니다.

```
#service  smb start
```

－ 봉사의 중지

화일공유봉사기(Samba Server)는 다음의 지령에 의하여 중지시킵니다.

```
#service  smb stop
```

2) 사용방법

화일공유봉사기(Samba Server)를 리용하는데서 크게 Samba사용자관리방법과 봉사설정관리방법 및 기타 편의쏘프트웨어들에 대한 리용방법을 설명합니다.

(1) Samba사용자관리(생성, 삭제, 암호설정)

－ Samba사용자생성 및 암호설정

Samba사용자를 새로 생성하기전에 체계사용자부터 먼저 생성하여야 합니다. 체계사용자는 adduser지령을 리용하여 생성합니다.

다음 이렇게 생성한 사용자를 Samba사용자로 전환시켜 새로운 Samba사용자를 생성합니다. Samba사용자로 전환하는 지령은 다음과 같습니다.

smbpasswd –a 사용자이름

이 지령을 리용하면 새로 생성하는Samba사용자의 암호를 입력하기 위한 재촉확인문이 현시됩니다. Samba사용자의 암호를 두번 입력해주면 Samba사용자가 생성됩니다. 암호를 입력하지 않으려는 경우에는 Enter건을 리용하여 그대로 탈퇴합니다.

－ Samba사용자의 암호변경

Samba사용자의 암호변경 역시 smbpasswd지령을 리용합니다. 다만 사용자생성지령에서 선택항목 –a를 리용하지 않을뿐입니다.

root사용자의 암호를 변경하려는 경우에는 smbpasswd지령을 그대로 리용하며 기타 사용자의 암호를 변경하려면 사용자이름을 파라메터로 주어야 합니다.

smbpasswd 사용자이름

- Samba사용자의 사용허가 및 금지

Samba사용자를 리용하지 못하도록 일시적으로 사용을 금지시킬수도 있습니다. Samba사용자를 사용금지시키기 위해서는 다음과 같은 지령을 실행시킵니다.

smbpasswd –d 사용자이름

Samba사용자가 사용금지되였다고 하여 그 사용자 자체가 삭제되는것은 아닙니다. 다만 그 사용자를 리용할수 없을뿐입니다.

금지된 Samba사용자를 다시 리용할수 있게 사용허가시키려면 다음과 같은 지령을 실행합니다.

smbpasswd –e 사용자이름

Samba사용자의 사용금지 및 허가지령은 root사용자만이 가능합니다. 기타 사용자들은 이 지령을 실행시킬수 있는 권한을 가지고있지 않습니다.

- Samba사용자의 삭제

Samba사용자를 완전히 삭제하려면 다음과 같은 지령을 실행합니다.

smbpasswd –x 사용자이름

이 지령을 실행하면 등록된 사용자를 삭제합니다.

이 지령도 역시 root사용자만이 실행시킬수 있는 권한을 가지고있습니다.

(2) 화일공유봉사기(Samba Server)의 구성화일설정을 변경

Samba봉사기의 기본설정정보는 /etc/samba/smb.conf화일에 등록되여있습니다. 이 화일의 정보를 변경시키는 방법으로 Samba봉사기의 설정을 변경시킬수 있습니다.

이 화일을 변경시킨 후에 testparm지령을 리용하여 smb.conf화일의 문법적합성을 검증해볼수 있습니다.

smb.conf화일은 크게 “일반설정”, “자동사용자등록부”, “인쇄기설정”과 같은 3가지 요소로 구성되여있습니다.

여기서 “일반설정”부분은 Samba봉사기가 공유하는 자원들에 공통적으로 적용하려는 기본값들을 설정하는부분입니다. 만약 여기서 설정한 값과 개별사용자의 사용자등록부에서 설정한 값이 중복된다면 개별사용자의 설정값이 우선권을 가집니다. 이 설정은 [global]이라는 선언으로 시작됩니다.

“자동사용자등록부”부분은 체계사용자들의 사용자등록부를 사용자가입등록부로 사용하기 위한 설정부분입니다. 이 설정은 [homes]이라는 선언으로 시작됩니다.

“인쇄기설정”부분은 망공유인쇄기에 대한 설정부분으로서 [printers]로 시작하는 부분입니다.

이 외에도 개별적인 사용자들마다 해당한 봉사설정을 진행하도록 하기 위하여 여러개의 [ ]기호들을 추가할수 있습니다.

– 일반설정
  - Unix charset = cp949 : Unix문자모임을 설정
  - dos charset = cp949 : dos문자모임을 설정
  - display charset = cp949 : 화면문자모임을 설정
  - workgroup = MYGROUP : NT령역이름 또는 작업집단이름을 지정합니다.
  - server string = Samba Server Version 3.5 : Samba봉사기의 이름으로서 용도에 맞게 설정할수 있습니다.
  - hosts allow = 192.168.1.192.168.2.127. : Samba봉사기의 보안을 위하여 매우 중요한 추가선택입니다. Samba봉사기로의 접근을 허용하기 위한 설정으로서 실례에서는 192.168.1.망과 192.168.2.망 그리고 국부주콤퓨터에서의 접근을 허용하는 설정실례입니다. 이외에도 다양한 설정이 가능합니다.
  - load printers = yes : 자동인쇄목록을 사용하기 위한 값으로 yes라고 주면 망인쇄기를 Samba봉사기에서 관리하도록 하겠다는 의미를 가집니다.
  - printcap name = /etc/printcap : printcap화일의 위치가 다른곳에 있다면 그곳을 지정합니다.

- printing = bsd : 사용하는 인쇄기가 표준이 아니라면 주석처리를 해두는것이 좋습니다. 현재 지원하는 인쇄체계의 종류로는 bsd, sysv, plp, lprng, aix, hpux, qnx등이 있습니다.
- guest account = pcquest : Samba봉사기의 guest사용자를 허용하자고 할때에는 이 주석을 제거해야 합니다. 즉 이 추가선택은 Samba봉사기에 guest권한으로 접속하였을 때 어떤 권한을 부여할것인가를 설정하는것입니다. 가능한 체계에 특별한 권한이 없는 nobody 와 같은 권한으로 설정해주는것이 좋습니다. 만약 nobody를 설정하지 않으려면 useradd 명령으로 /etc/passwd에 guest권한으로 사용할 권한을 생성한 후에 그 권한을 설치하여야 합니다.
- log file = /var/log/samba/log.%m : Samba봉사기로 접속하는 개별사용자들의 주콤퓨터정보를 %m으로 받아서 개별리력화일을 생성하도록 합니다. 주콤퓨터별로 리력화일을 사용하지 않는다면 하나의 리력화일 /var/log/smaba/log.smbd를 사용할수도 있습니다. 이 화일에 Samba접속리력을 모두 기록하게 됩니다.
- max log size = 50 : 리력화일의 용량크기를 KB단위로 제한하기 위한 추가선택입니다. 우의 실례는 50KB로 제한한 실례이며 만약 제한하지 않으려면 0을 입력합니다.
- security = share : 보안방식을 설정하는것으로서 대부분의 Samba접속자들에게는 user준위가 가장 알맞습니다. 즉 user준위를 설정하면 Samba봉사기에 접속하는 사용자는 반드시 Windows에서 사용하는 사용자가입ID와 동일해야 합니다. 만약 우의 설정과 같이 share준위를 설정하면 공유등록부등에 설정하는것으로서 ID와 암호의 인증없이 접속하는것을 허용하는 준위입니다. 또한 server준위는 별도의 인증봉사기에서 ID와 암호인증을 받도록 하는 준위입니다. 가능한다면 Samba봉사기보안을 위하여 user준위를 사용하는것이 좋습니다.
- password server = <NT-Server-Name> : security 추가선택값이 server로 설정되였을 때에만 설정할수 있는 추가선택으로서 인증봉사기로 사용할 봉사기를 지정합니다.

- password level = 8 : 암호문자로 대소문자를 조합하여 사용할 문자의 개수를 지정한 추가선택입니다.
- username level = 8 : Samba사용자명을 대소문자조합하여 사용할 문자의 개수를 지정한 추가선택입니다.
- encrypt passwords = yes : 암호를 암호화하여 사용하려면 “encrypt passwords” 추가선택값을 yes로 설정하여야 합니다.
- Unix password sync = Yes
- passwd program = /usr/bin/passwd %u
- passwd chat = *New*UNIX*password* %n\n *ReType*new*UNIX*password* %n\n
- *passwd:&all*authentication*tokens*updated*successfully* : Samba사용자가 원격지에서 Samba암호를 변경할수 있도록 허용하도록 하는 설정입니다. 암호를 변경하도록 허용하려면 앞의 encrypt passwords추가선택값에 yes라고 해야 하고 smb passwd file추가선택에 반드시 Samba사용자암호화일의 경로를 지정해야 합니다.
- username map = /etc/samba/smbusers : 대부분 Samba에서 사용하는 ID와 Linux권한 ID는 동일하게 사용합니다. 만약 Samba사용자이름과 Linux권한사용자이름을 다르게 사용할 경우에 이를 대응할수 있도록 하기 위한 추가선택으로서 대응표화일을 /etc/samba/smbusers화일로 사용하는 설정입니다.
- include = /etc/samba/smb.conf.%m : Samba접속자의 가동환경에 따라서 각기 다른 설정화일을 적용할수 있도록 지원하기 위해 사용하는 추가선택입니다. %m은 접속자체계의 NetBIOS이름으로 대체되여 접속한 사용자의 가동환경종류에 따라서 각기 다른 Samba설정화일을 적용할 수 있습니다.
- socket options = TCP_NODELAY SO_RCVBUF=8192 SO_SNDBUF=8192 : Samba봉사의 성능향상을 위한 추가선택입니다.
- interfaces = 192.168.12.2/24 192.168.13.2/24 : Samba봉사기에서 두개이상의 망대면부(NIC)를 사용하도록 지원하기 위한 추가선택입니다.

Samba봉사기가 사용하는 모든 대면부의 망대역을 설정해야만 그 망대면부를 사용할수 있도록 합니다.

- remote browse sync = 192.168.3.25 192.168.5.255
- remote announce = 192.168.1.255 192.168.2.44 : 지역부분망에서 Samba봉사기를 잘 인식하도록 하기위하여 자기자신을 알리도록 합니다.
- local master = no : 이 추가선택은 특정부분망내에서 Samba봉사기가 국부기본열람기가 되도록 하는 추가선택입니다.
- os level = 33 : 기본열람기선출(master browser elections)에서 이 봉사기의 우선권을 가질수 있도록 허용합니다.
- domain master = yes : Samba봉사기를 Windows 95기반의 콤퓨터에 대한 령역사용자가입봉사기역할을 하도록 하려면 이 추가선택을 사용하여야 합니다.
- logon script = %m.bat : 매개 가동환경 또는 사용자별로 사용자가입스크립트를 구분하여 사용할수 있도록 합니다.
- logon script = %U.bat : 사용자별로 사용자가입묶음화일을 지정하여 사용할수 있도록 합니다.
- logon path = \\%L\Profiles\%U : 오직 Windows 95 또는 Windows NT에서 roving profile을 어디에 저장해둘것인가를 지적하는 설정입니다.
- wins support = yes : Windows 인터네트이름봉사인 WINS를 지원하기 위한 부분입니다.
- wins server = w.x.y.z : WINS봉사기를 지정하기 위한 추가선택입니다.
- wins proxy = yes : wins프록시(WINS)기능이 없는 의뢰기대신 질문에 대답하기 위한 추가선택입니다.
- dns proxy = no : NDS의 nslookup을 사용하여 NetBIOS이름을 찾을것인가 아닌가를 지정하는 추가선택입니다.
- preserve case = no
- short preserve case = no : 대소문자를 유지보존할것인가를 지정하는 추가선택입니다. 체계의 기본값은 no입니다. 이 설정은 각 공유마다 별도로 설정할수 있습니다.

- default case = lower : DOS화일들의 기본문자는 대문자로 인식합니다. 만약 lower로 설정한다면 소문자로 인식합니다.
- case sensitive = no : 대소문자의 구분을 할것인가 말것인가를 지정하는 추가선택입니다.

– 자동사용자등록부 설정

기본적인 표준설정값은 다음과 같습니다.

```
[home]
comment = Home Directories
broseable = no
writable = yes
```

령역사용자가입기능을 사용하려면 netlogon설정을 진행하여야 합니다.

```
[net logon]
 comment = Network Logon Service
 path = /home/netlogon
 guest ok = yes
 writable = no
 share modes = no
```

Smb사용자들의 림시공유등록부로 사용하기 위한 설정은 다음과 같습니다.

```
[tmp]
 comment = Temporary file space
 path = /tmp
 read only = no
 public = yes
```

Smb사용자라면 누구나 다 접근이 가능한 공유등록부로서 staff집단에 등록된 사용자들을 제외한 일반사용자들은 읽기 전용으로만 사용할수 있게 하려면 다음과 같이 설정하여야 합니다.

```
[public]
 comment = Public Stuff
 path = /home/samba/public
 public = yes
```

```
read only = no
write list = @staff
```

공유등록부로 사용할 위치를 지정하고 staff집단에 등록된 사용자를 제외한 나머지 일반사용자들은 모두 읽기전용으로만 접근하게 하려면 다음과 같이 설정합니다.

```
[public]
 path = /usr/somewhere/else/public
 public = yes
 only guest = yes
 writable = yes
 printable = no
```

gusle이라는 smb사용자를 위한 특별설정은 다음과 같습니다.

```
[gusle]
 comment = gusle USER
 path = /home/gusle
 valid users = gusle
 read only = no
 writable = yes
 public = no
 browseable = yes
 printable = no
 create mask = 0750
```

- 인쇄기 설정

BSD형태의 인쇄체계를 가지고있다면 개별설정없이 바로 사용할수 있습니다. 아래에서와 같이 guest ok항목이 yes로 되여있다면 guest권한으로 지정한 사용자들이 이 인쇄체계를 사용할수 있습니다.

```
[printers]
 comment = All Printers
```

path = /var/spool/samba

browseable = no

guest ok = yes

writable = no

printable = yes

(3) 기타 편의쏘프트웨어

－ Samba봉사기의 사용자가입정보확인을 위한 smbstatus

현재 Samba봉사기로 사용자가입하여 사용하고있는 사용자들의 정보를 확인할수 있는 Samba관리자명령입니다. 간단히 현재 Samba봉사기에 련결된 사용자들의 목록을 확인하는 명령어입니다.

위치 : /usr/bin/smbstatus

사용형식 : smbstatus [-P][-b][-d][-L][-p][-S][-s <설정화일>][-u smb권한]

이 지령은 Samba봉사기관리자가 주로 실행하며 현재 어떤 사용자들이 봉사기에 가입하여 사용하고있는가를 확인하려고 할 때 리용합니다.

－ Smb설정화일점검을 위한 testparm

위치 : /usr/bin/testparm입니다.

사용형식 : testparm [-s][-h][-x][-L<봉사기이름>]설정화일이름[주콤퓨터이름 IP]

이 지령을 파라메터가 없이 실행하면 현재의 smb.conf화일전체를 점검합니다. 도중에 “Press enter to see a dump of your service definitions”가 출력되고 일단 중지됩니다. 이상이 없으면 “OK”를 출력한 후에 smb의 개별봉사정의부분을 출력하려면 ENTER건을 입력하라는 통보가 나옵니다. 만약 이상이 있다면 이상발견내용을 알려주게 됩니다.

원격봉사기의 smb봉사기설정화일도 점검할수 있습니다.

testparm –L 172.29.88.100

제8절. 화일전송봉사기(VSFTP Server)

이 절에서는 《붉은별》 봉사기용체계 3.0에서 화일전송봉사기(VSFTP Server)를 설치운영하기 위한 방법을 설명합니다.

1. 화일전송봉사기 개요

대단히 안전한 화일전송규약(Very Secure File Transfer Protocol)은 TCP/IP환경에서의 화일전송용응용쏘프트웨어통신규약이며 이를 실현한 쏘프트웨어를 설치한 봉사기가 화일전송봉사기(VSFTP Server)입니다.

화일전송봉사기(VSFTP Server)는 구성화일과 관리대몬, 인증화일들, 안내페지와 실행에 필요한 서고화일들로 구성되여있습니다.

참고 : 화일전송봉사기(VSFTP Server)가 비정상적으로 동작하는 경우 구성화일을 여벌복사한 상태에서 봉사패키지를 해제하고 다시 설치한 다음 여벌복사한 구성화일을 다시 해당한 위치에 복사하여 봉사를 재구성하여야 합니다.

2. 화일전송봉사기 설치

화일전송봉사기(VSFTP Server)는 우리 식 조작체계《붉은별》 봉사기용체계 3.0이 설치될 때 자동적으로 설치됩니다.

vsftp패키지를 수동적으로 설치하는 경우에는 먼저 vsftpd-2.2.2-6.RSS3.i686.rpm패키지가 설치되여있는가를 확인하여야 합니다. 이 패키지들이 없으면 vsftp를 설치될수 없으며 강제적으로 설치한다고 해도 vsftp대몬이 정확히 실행될수 없습니다.

지령행에서 해당 패키지들이 설치되였는가를 확인합니다.

```
#rpm –qa | grep vsftp
vsftpd-2.2.2-6.rss3
```

우와 같은 결과가 나오지 않으면 이 패키지들이 설치되지 않은것이므로 설치하여야 합니다.

CD 를 리용하여 설치를 진행하는 경우에는 먼저 CD 구동기에 《붉은별》 봉사기용체계 3.0 CD 를 넣고 탑재를 시켜야 합니다.

```
# mount /dev/cdrom /mnt/cdrom
```

패키지들이 들어있는 등록부에서 설치하려는 패키지들이 있는가를 확인합니다. 확인이 끝나면 설치를 시작합니다.

3. 화일전송봉사기의 작업절차

1) 화일전송봉사기의 봉사시작과 중지, 재시작

- 봉사의 시작
  #service vsftpd start

- 봉사의 중지
  #service vsftpd stop

- 봉사의 재시작
  #service vsftpd restart

rpm 으로 설치된 vsftp 봉사기의 시작, 중지, 재시작과 같은 실행조종을 위해서 리용되는 방법에는 크게 2 가지 방식이 있습니다.

실행방법에는 독립실행방식과 xinetd 방식이 있으며 기정으로 독립실행방식으로 동작합니다.

독립실행방식은 21 번포구를 할당한 후 대기하다가 말단요청이 들어오면 직접 요청을 받아 응답하는 형태로 처리하는 방식이며 xinetd 방식은 ftp 봉사기대신에 21 번포구를 열고 대기하다가 말단요청이 들어오면 ftp 봉사기를 실행시키는 방식입니다.

인터네트봉사쏘프트웨어인 xinetd 를 리용하여 vsftpd 봉사를 실행하는 경우에는 설정화일인 /etc/vsftpd/vsftpd.conf 화일의 파라메터 listen 이 no 로 되여있어야 합니다.

Xinetd 방식으로 대몬을 실행시키기 위하여 Xinetd 봉사화일을 만들어주어야 합니다. 하지만 rpm 패키지를 통하여 vsftp 를 설치하는 경우에는 이미 /usr/share/doc/vsftpd-2.2.2/vsftpd.xinetd 화일이 존재하기때문에 이 화일을 /etc/xinetd.d/등록부의 vsftpd 화일로 복사해서 사용하면 됩니다.

#cp /usr/share/doc/vsftpd=2.2.2/example/internet_site/vsftpd.xinitd etc/xinitd.d/vsftpd

xinetd 로 동작할수 있도록 vsftpd 화일을 수정합니다. 이미의 편집기로 /etc/xinet.d/vsftpd 화일을 열고 disable =no 로 설정되였는가를 확인합니다.

다음 다음의 행을 수정해야 합니다.

Server=/usr/local/sbin/vsftpd 를 server=/usr/sbin/vsftpd 로 수정합니다.

다음의 행을 새로 추가해야 합니다.

Server_agrs=/etc/vsftpd/vsftpd.conf

화일갱신이 완료되면 xinetd 대몬을 재실행시킵니다. Xinetd 대몬은 포구 21 을 열고 대기하다가 ftp 요청이 들어올 때 vsftpd 대몬을 실행시켜줍니다.

#service xinitd restart

2) 화일전송봉사기의 구성화일설정

/etc/vsftp/ vsftp.conf 는 vsftp 봉사기의 기본구성화일입니다.
이 화일을 임의의 편집기로 열고 매 항목들에 대한 설정을 진행합니다.
항목들에 대한 설명은 다음과 같습니다.

① vsftpd 가 닉명사용자의 가입을 접수하는 경우 anonymous_enable 값을 YES 로 설정합니다.

② 국부사용자들의 접속을 허용하는 경우 Local_enable 값을 YES 로 설정합니다. 기정값은 YES 이며 NO 로 설정하는 경우 국부사용자계산자리의 접속을 거부합니다.

③ 사용자가 ftp 봉사기에 화일을 올리적재하는것을 허용하는 경우 write_enable 값을 YES 로 설정합니다. 기정값을 NO 입니다.

④ 닉명의 사용자들이 닉명의 사용자가 쓰기권한을 가지고있는 등록부안에 화일들을 올리적재하게 하려면 anon_upload_enable 과 write_enable 이 둘다 YES 로 되여야 합니다.

⑤ 닉명의 사용자들이 닉명의 사용자가 쓰기권한을 가지고있는 등록부내에 등록부를 창조하게 하려면 anon_mkdir_write_enable 와 write_enable 이 둘다 YES 로 설정되여야 합니다.

⑥ 닉명의 사용자들이 닉명의 사용자가 쓰기권한을 가지고있 등록부내에서 등록부이름변경과 삭제를 진행하게 하려면 anon_other_write_enable 와 write_enable 이 둘다 YES 로 설정되여야 합니다.

⑦ 닉명의 사용자들이 읽을수 없는 화일을 내리적재하는것을 금지하려면 anon_world_readable_only 값을 YES 로 설정하여야 합니다.

⑧ 일반적으로 vsftpd 는 /var/log/vsftpd.log 에 기록통보문을 씁니다. syslog_enable 값을 YES 로 설정하는 경우 통보문들을 체계의 syslog 봉사에 보냅니다.

⑨ 하나의 원천 IP 주소에서 허가되는 동시접속수의 최대수를 지정하려면 max_per_ip 값을 설정하여야 합니다.

⑩ ftp 접속 후 화일갱신과 내리적재에 대한 기록을 남길것인가(yes) 남기지 않을것인가(no)를 설정하려면 Xferlog_enable 값을 설정하여야 합니다.

⑪ ftp 기록화일의 위치를 결정하려면 Xferlog_file 값을 설정하여야 합니다.Vsftp 는 기본적으로 /var/log/vsftpd.log 화일을 기본기본화일로 사용합니다.

⑫ 기록화일에 남길 기록화일의 형식(format)을 기본형식으로 남길것인가(yes) 아닌가(no)를 결정하려면 Xferlog_std_format 값을 설정하여야 합니다.
⑬ ftp 련결에서 idle 시간에 대한 시간초과값을 설정하려면 Idle_session_timeout 값을 설정하여야 합니다.
⑭ 자료전송시 적용되는 시간초과값을 설정하려면 Data_connection_timeout 값을 설정하여야 합니다.
⑮ ftp 봉사의 전송속도를 제한하려면 Trans_chunk_size 값을 설정하여야 합니다. 초당바이트수를 지정할수 있으며 제한없이 허용하려면 0으로 설정하면 됩니다. 이 설정은 vsftpd 가 독립대몬방식으로 봉사될 때에만 적용됩니다.
⑯ vsftpd 를 xinetd 방식이 아닌 독립대몬으로 봉사하려면 listen 값을 YES 로 설정한 상태에서 Listen_port 값을 21로 지정합니다.

vsftpd.1conf 화일을 변경한 다음에는 반드시 봉사기를 재시작하여야 합니다.

제9절. 망인증봉사기(kerberos)

이 절에서는 kerberos 봉사를 진행하기 위한 kerberos 봉사기 및 kerberos 의뢰기들의 구성방법을 설명합니다.

1. 망인증봉사기의 개요

1) kerberos 란

Kerberos 는 봉사기와 의뢰기사이의 상호인증을 보장하는 망인증규약이며 대칭열쇠암호화를 리용하여 망봉사들에 대한 사용자인증을 진행합니다.

《붉은별》 봉사기용체계 3.0 에 포함된 kerberos 봉사기는 KerberosV 를 실현한 쏘프트웨어로서 판본은 1.8.2 입니다.

Kerberos 봉사기를 운영하기 위해서는 kerberos 를 리용하기 위한 관리령역을 정의하고 kerberos 봉사기를 구성하여야 하며 관리령역내의 봉사기와 의뢰기들이 kerberos 를 리용하여 봉사를 진행하거나 봉사받도록 설정해야 합니다.

2) 사용목적

망에서의 체계보안과 완전성은 다루기 힘들수 있습니다. 망에서 어떤 봉사들이 실행되고있고 이 봉사들이 어떤 방식으로 리용되는가를 추적하는것은 관리자들에게 많은 시간을 요구합니다. 더우기 망봉사에 대한 사용자인증은 규약이 리용하는 방법이 본래 안전하지 못할 때 위험할수 있습니다. 이것은 통과암호들

을 암호화하지 않고 망으로 전송하는 전통적인 FTP 와 Telnet 규약들이 잘 보여주고있습니다.

Kerberos 는 안전치 못한 인증방법들을 허용하는 규약들을 위한 방법이며 그에 의하여 전반적인 망보안을 강화합니다.

Kerberos 는 MIT 가 만든 망인증규약이며 대칭열쇠암호화를 리용하여 망봉사들에 대한 사용자인증을 진행합니다. 이것은 통과암호들이 망을 통하여 사실상 절대로 보내지지 않는다는것을 의미합니다.

결과적으로 사용자들이 Kerberos 를 리용하여 망봉사들에 인증할 때 망통화를 감시하여 통과암호들을 수집하려고 시도하는 권한없는 침입자들을 효과적으로 차단할수 있습니다.

대부분의 관습적인 망봉사들은 통과암호에 기초한 인증방식을 리용합니다. 그러한 방식들은 사용자가 망봉사기에 자기의 사용자이름과 통과암호를 주어 인증할것을 요구합니다. 유감스럽게도 인증정보는 많은 봉사들에서 암호화되지 않고 전달됩니다. 그러한 방식들은 보호되려면 외부자들이 망에 접근할수 없어야 하고 망상의 모든 콤퓨터들과 사용자들은 서로 신뢰하고 신뢰받을수 있어야 합니다.

하지만 이러한 경우에도 인터네트와 련결된 망은 더 이상 안전하다고 가정할수 없습니다. 망에 대한 접근을 얻은 공격자는 파케트탐지기라고도 하는 간단한 파케트분석기를 리용하여 사용자이름과 통과암호들을 가로챌수 있으며 사용자 권한들과 전체 보안기반구조의 완전성을 위태롭게 할수 있습니다.

Kerberos 의 주요설계목적은 암호화되지 않은 통과암호가 망을 통하여 전송되는것을 없애는것입니다. 정확히 리용될 때 Kerberos 는 파케트탐지기가 망에 주는 위협을 효과적으로 제거할수 있습니다.

3) 용어 및 략어

Kerberos 는 여러가지 봉사기능들을 정의하기 위해 자체의 용어들을 가지고있습니다. Kerberos 가 어떻게 동작하는가를 알기전에 다음의 용어들을 익혀두는것이 중요합니다.

인증봉사기 authentication server (AS)

봉사에 접근하려는 사용자들에게 요청한 봉사에 대한 허가증(ticket)들을 발급하는 봉사기입니다.

AS 는 증명서가 없거나 받지 못한 의뢰기로부터의 요청에 응답합니다. 인증봉사기는 보통 허가증발급허가증(ticket-granting ticket (TGT))를 발급함으로써 허가증발급봉사기(ticket-granting server (TGS))봉사에 대한 접근을 얻는데 리용됩니다. AS 는 보통 열쇠배포중심(key distribution center (KDC))과 같은 주콤퓨터상에서 실행됩니다.

암문 ciphertext

암호화된 자료.

의뢰기 client

Kerberos 로부터 허가증을 받을수 있는 망상의 실체(사용자, 주콤퓨터, 응용쏘프트웨어) 입니다.

증명서 credentials

특정한 봉사에 대해서 의뢰기의 신분을 확인하는 전자증명서들의 립시모임. 허가증이라고도 합니다.

증명서고속완충기억기 또는 허가증화일 credential cache or ticket file

사용자와 여러가지 망봉사들사이에 통신을 암호화하기 위한 열쇠를 포함하는 화일입니다.

Kerberos 5 는 공유기억기와 같은 다른 고속완충기억기형태를 리용한 흐레임워크를 지원하지만 보다 철저하게는 화일을 지원합니다.

암호해쉬 crypt hash

사용자들을 인증하는데 리용되는 한방향해쉬입니다.

이것들은 암호화되지 않은 자료를 리용하는것보다는 안전하지만 여전히 경험있는 공격자들이 해독하기가 상대적으로 쉽습니다.

GSS-API

Generic Security Service Application Program Interface (Internet Engineering Task Force 가 발표한 RFC-2743 에 정의)는 보안봉사들을 제공하는 함수들의 모임입니다. 이 API 는 의뢰기와 봉사들이 서로 인증하는데 리용되며 기본적인 방식은 몰라도 됩니다. 만약 어떤 망봉사(례로 cyrus-IMAP)가 GSS-API 를 리용한다면 그것은 Kerberos 를 리용하여 인증할수 있습니다.

해쉬 hash

해쉬값이라고도 합니다. 해쉬함수에 문자렬을 넘김으로써 생성되는 값입니다. 이 값들은 대체로 전송된 자료가 부당하게 변경되지 않았는가를 확인하는데 리용됩니다.

해쉬함수 hash function

입력자료로부터 수자적인 《지문》을 생성하는 방법입니다.

이 함수들은 자료를 재배치하거나 바꾸어넣거나 변경하여 해쉬값을 생성합니다.

열쇠 key

다른 자료를 암호화하거나 복호화할 때 리용되는 자료.

암호화된 자료는 정확한 열쇠나 공격자에게 최대의 행운이 없이는 복호화될수 없습니다.

열쇠배포중심 key distribution center (KDC)

Kerberos 허가증들을 발급하는 봉사이며 보통 허가증발급봉사기(TGS)와 같은 주콤퓨터상에서 실행됩니다.

열쇠표 keytab (or key table)

암호화되지 않은 기본실체(principal)들과 그의 열쇠들의 목록이 들어있는 화일입니다.

봉사기들은 kinit 를 리용하는 대신 keytab 화일로부터 필요한 열쇠를 검색합니다. 기정 keytab 화일은 /etc/krb5.keytab 입니다. KDC 관리봉사기 /usr/kerberos/sbin/kadmind 는 다른 화일을 리용하는 유일한 봉사입니다.(그것은 /var/kerberos/krb5kdc/kadm5.keytab 를 리용합니다.)

kinit

kinit 지령은 이미 가입한 기본실체가 초기 허가증발급허가증(TGT)을 얻어 고속완충기억기할수 있게 합니다. 구체적인 정보는 kinit 안내페지를 참고하십시오.

기본실체 principal (또는 principal name)

기본실체는 Kerberos 를 리용하여 인증이 허용되는 사용자나 봉사의 유일한 이름입니다. 기본실체는 형태 root[/instance]@REALM 를 따릅니다. 전형적인 사용자에 대하여 root 는 그의 가입 ID 와 같습니다. Instance 는 선택적입니다. 만약 기본실체가 instance 를 가진다면 그것은 root 와 ("/")로 분리됩니다. 빈 문자렬("")은 유효한 instance(기정 NULL instance 와 다른)로 여기지만 그것을 리용하면 혼동할수 있습니다. 관리령역내에서 모든 기본실체들은 자체의 열쇠를 가지는데 이것은 사용자들에 대하여 통과암호로부터 얻어지거나 봉사들에 대하여 우연적으로 설정됩니다.

관리령역 realm

Kerberos 를 사용하는 망이며 KDC 라고 하는 하나이상의 봉사기들과 많은 수의 의뢰기들로 이루어집니다.

봉사 service

망을 통하여 호출되는 쏘프트웨어입니다.

허가증 ticket

특정한 봉사에 대하여 의뢰기의 신분을 조사하는 전자증명서들의 림시모임. 증명서라고도 합니다.

허가증발급봉사기 ticket-granting server (TGS)

봉사에 접근하려는 사용자들에게 요청한 봉사에 대한 허가증들을 발급해주는 봉사기입니다.

TGS 는 보통 KDC 와 같은 주콤퓨터상에서 실행됩니다.

허가증발급허가증 ticket-granting ticket (TGT)

의뢰기가 KDC 에 요청하지 않고 추가적인 허가증들을 얻을수 있도록 하는 특별한 허가증입니다.

2. 망인증봉사기의 설치

1) 화일목록

Kerberos 봉사기는 kerberos 쏘프트웨어(krb5-server-1.8.2, krb5-libs-1.8.2, krb5-pkinit-openssl-1.8.2, krb5-workstation-1.8.2, krb5-appl-clients-1.0.1-1 패키지)가 설치되여야 합니다.

Kerberos 의뢰기는 kerberos 서고 및 의뢰기쏘프트웨어(krb5-libs-1.8.2, krb5-pkinit-openssl-1.8.2, krb5-workstation-1.8.2, krb5-appl-clients-1.0.1-1 패키지)가 설치되여야 합니다.

2) 쏘프트웨어의 구성관계

Kerbero 인증체계는 기본적으로 kerberos 서고와 kerberos 인증봉사기 및 응용쏘프트웨어봉사기, kerberos 의뢰기로서 구성되며 이것은 krb5-libs, krb5-server, krb5-pkinit-openssl, krb5-workstation, krb5-appl-server, krb5-appl-clients 의 패키지들로 이루어집니다.

krb5-libs 실행패키지는 Kerberos 5 에 필요한 공유서고들을 포함합니다. 이 패키지는 kerberos 의 열쇠배포중심(kdc), 관리봉사기(kamdin), 자료기지편의프로그람, kerberos 의뢰기 및 응용쏘프트웨어들이 리용하는 kerberos 인증기능들과 암호화모듈들이 들어있는 kerberos 서고(libkrb5) 와 kerberos 자료기지관리서고(libkdb5), kerberos 관리봉사서고 (libad m5srv)를 포함하고있습니다. Kerberos 를 리용하려면 이 패키지를 설치하여야 합니다.

krb5-server 패키지는 열쇠배포중심(kdc), 관리봉사기(kamdin), kerberos V5 와 V4 호환봉사 krb524 를 포함하고있는 Kerberos 5 의 봉사기쏘프트웨어입니다. Kerberos 5 봉사기를 설치하려면 이 패키지를 설치하여야 합니다.

krb5-workstation 패키지는 의뢰기들에서 Kerberos 5 를 리용하기 위한 쏘프트웨어들을 포함합니다. krb5-workstation 패키지는 Kerberos 허가증관리쏘프트웨어들(kinit, klist, kdestroy, kpasswd)과 의뢰기에서 자료기지에 접속하기 위한 쏘프트웨어(kadmin) 등을 포함합니다. 망에서 Kerberos 를 리용하려면 이 패키지를 매 의뢰기들에 설치하여야 합니다.

krb5-appl-server 패키지는 Telnet 와 FTP 의 Kerberos 화된 판본(krb5-telnet, gssftp)들을 비롯하여 kerberos 인증체계를 리용하는 봉사기대몬 쏘프트웨어들을 포함하고있습니다. 망에서 Kerberos 화된 봉사대몬들을 봉사하려면 이 패키지를 응용봉사기에 설치하여야 합니다.

3) 쏘프트웨어의 설치

《붉은별》 봉사기용체계 3.0 에는 기정으로 Kerberos 쏘프트웨어가 설치되여 있습니다. 즉 krb5-server-1.8.2, krb5-libs-1.8.2, krb5-pkinit-openssl-1.8.2, krb5-workstation-1.8.2, krb5-appl-clients-1.0.1-1 패키지들이 기정적으로 설치됩니다.

Kerberos 를 리용하려면 모든 봉사기 및 의뢰기들에 krb5-libs, krb5-pkinit-openssl, krb5-workstation-1.8.2 패키지를 설치하여야 합니다.

Kerberos 5 봉사기에는 추가적으로 krb5-server 패키지를 설치하여야 합니다.

Kerberos 화된 봉사대몬들을 봉사하는 봉사기들에는 추가적으로 krb5-appl-server 패키지를 설치하여야 합니다.

Kerberos 봉사를 받는 의뢰기들에는 krb5-appl-clients 패키지를 설치하여야 합니다.

3. 망인증봉사기의 동작방식과 구축하기

1) 봉사의 시작과 중지

kerberos 봉사기를 사용하기 위해서는 kerberos 관리령역을 정의하고 kerberos 봉사기구성정보를 편성해야 합니다. (2) 동작방식을 참고할것)

kerberos 봉사대몬(krb5kdc, kadmin)들이 기동되여있는 경우 대몬중지 지령(service servicename stop)으로 봉사대몬들을 중지시킵니다.

2) 동작방식의 개요

Kerberos 는 사용자이름/통과암호 인증방법들과 다르다. 모든 망봉사에 모든 사용자를 인증하는 대신에 Kerberos 는 대칭암호화와 신뢰되는 3 자(KDC)를 리용하여 어떤 망봉사묶음에 사용자들을 인증합니다. 사용자가 KDC 에 인증할 때 KDC 는 사용자의 콤퓨터에로 그 대화접속에 특정한 허가증을 보내며 Kerberos 화된 봉사들은 사용자가 통과암호를 리용하여 인증할것을 요구하는것이 아니라 사용자의 콤퓨터상에서 허가증을 찾습니다.

Kerberos 화된 망의 사용자가 자기 작업기에 가입할 때 그의 기본실체는 인증봉사기로부터 TGT 에 대한 요청의 한 부분으로서 KDC 에 전송됩니다. 이 요청은 사용자의 특별한 조작없이 log-in 쏘프트웨어에 의해서 전송되거나 사용자가 가입한 후에 kinit 쏘프트웨어로 보낼수 있습니다.

그러면 KDC 는 자기의 자료기지에서 그 기본실체를 검사합니다. 기본실체가 발견되면 KDC 는 사용자의 열쇠로 암호화된 TGT 를 작성하여 그것을 사용자에게 보냅니다.

그 다음 의뢰기의 login 이나 kinit 쏘프트웨어는 사용자의 열쇠를 리용하여 TGT 를 복호화하는데 이 열쇠는 사용자의 통과암호로부터 계산됩니다. 사용자의 열쇠는 오직 의뢰기에서만 리용되며 망을 통하여 전송되지 않습니다.

경고: Kerberos 체계는 망의 사용자가 Kerberos 화되지 않은 봉사에 통과암호를 평문으로 전송하여 인증한다면 위태로울수 있습 니다.
Kerberos 화되지 않은 봉사는 될수록 리용하지 말아야 합니다. 그러한 봉사들에는 Telnet 와 FTP 가 있습니다. 그러나 비록 리상적이지 않아도 SSH 나 SSL 로 보호된 봉사들과 같은 다른 암호화된 규약들을 리용하는것이 더 좋습니다

주의: Kerberos 는 정확히 동작하기 위해서 다음의 망봉사들에 의존합니다.
망상의 콤퓨터들사이의 대략적인 시간동기화.
망에 ntpd 와 같은 시간동기쏘프트웨어를 설치하여야 합니다.
망시간규약봉사기설정에 대한 구체적인 내용은 /usr/share/doc/ntp-<version-number>/index.html 을 참고하십시오 (여기서 <version-number>는 사용자의 체계에 설치된 ntp 패키지의 판번호입니다).
령역이름봉사 (DNS).
망의 DNS 항목들과 주콤퓨터들이 모두 정확히 구성되였는가를 확인해야 합니다. 구체적인 내용은 /usr/share/doc/krb5-server-<version-number>의 Kerberos V5 체계관리자안내서를 참고하십시오(여기서 <version-number>는 사용자의 체계에 설치된 krb5-server 패키지의 판번호입니다).

TGT 는 일정한 시간(보통 10~24 시간) 후에 유효기간이 끝나는것으로 설정되며 의뢰기의 증명서고속완충기억기에 보관됩니다. 유효기간이 끝나는 시간은 TGT 가 공격당하는 경우 공격자가 짧은 시간동안밖에 리용할수 없도록 설정됩니다. TGT 가 발급된 후에 사용자는 TGT 가 유효기간이 끝날 때까지 혹은 탈퇴하여 다시 가입할 때까지 자기의 통과암호를 다시 입력하지 않아도 됩니다.
사용자가 망봉사에 대한 접근을 요청할 때마다 의뢰기쏘프트웨어는 TGT 를 리용하여 TGS 로부터 지정된 봉사에 대한 새로운 허가증을 요청합니다. 그 다음 이 봉사허가증을 리용하여 그 봉사에 사용자를 인증합니다.

3) Kerberos5 봉사기 구축하기

Kerberos 5 의뢰기를 설정하는것은 봉사기설정보다 쉽습니다. 최소한 의뢰기 패키지들을 설치하고 매 의뢰기에 유효한 krb5.conf 구성화일을 주어야 합니다. ssh 와 slogin 이 의뢰기체계들에 원격으로 가입하는 한가지 좋은 방법인 동시에 rsh 와 rlogin 의 kerberos 화된 판본들도 리용할수 있습니다. 대신 이것은 몇가지 좀 더 많은 구성을 변경시켜야 합니다.

① Kerberos 의뢰기와 KDC 사이의 시간동기화가 제대로 되여있는가를 확인해야 합니다. 구체적인것은 앞의 Kerberos 5 봉사기구성내용을 참고하십시오. 또한 kerberos 의뢰기쏘프트웨어들을 구성하기전에 kerberos 의뢰기에서 DNS 가 정확히 동작하는가를 확인해야 합니다.
② 모든 의뢰기들에 **krb5-libs** 와 **krb5-workstation** 패키지들을 설치해야 합니다. 매 의뢰기들에 유효한 **/etc/krb5.conf** 화일(보통 이것은 KDC 에서 리용하는 **krb5.conf** 화일과 같을수 있습니다)을 주어야 합니다.
③ 관리령역의 작업기는 kerberos 자료기지에 자기의 주콤퓨터기본실체를 가져야 **ssh** 또는 kerberos 화된 **rsh** 나 **rlogin** 을 리용하여 접속한 사용자인증에 kerberos 를 리용할수 있습니다. **sshd**, **kshd**, **klogind** 봉사기쏘프트웨어들은 모두 주콤퓨터봉사의 기본실체에 대한 열쇠에 접근을 요구합니다. 추가적으로 kerberos 화된 **rsh** 나 **rlogin** 봉사들을 리용하려면 그 작업기에 **xinetd** 패키지가 설치되여야 합니다.

Kadmin 을 리용하여 KDC 에서 작업기에 대한 주콤퓨터기본실체를 추가합니다. 이 경우에 실체는 그 작업기의 주콤퓨터이름입니다. **Kadmin** 의 **addprinc** 지령에 **–randkey** 선택항목을 리용하여 기본실체를 작성하고 그것을 우연열쇠로 할당합니다.

addprinc –randkey host/*blah.example.com*

이제 기본실체가 작성되였으며 작업기자체에서 **kadmin** 을 실행하고 **kadmin** 의 **ktadd** 지령을 리용하여 작업기의 열쇠를 추출할수 있습니다.

ktadd –k /etc/krb5.keytab host/*blah.example.com*

④ 다른 kerberos 화된 망봉사들을 리용하기 위해서 **krb5-server** 패키지를 설치하고 봉사들을 시작하여야 합니다. 아래는 일부 일반적인 kerberos 화된 봉사들과 그것들을 가능하게 하는 명령들의 목록입니다.

- **ssh** – OpenSSH 는 의뢰기와 봉사기가 **GSSAPIAuthentication** 을 리용하도록 구성되였다면 GSS-API 를 리용하여 봉사기에 사용자를 인증합니다. 의뢰기도 **GSSAPIDelegateCredentials** 이 가능으로 되였다면 원격체계상에서 리용할수 있는 사용자 증명서가 작성됩니다.
- **Rsh** 와 **rlogin** – **rsh** 와 **rlogin** 의 kerberos 화된 판본을 리용하려면 **klogin**, **eklogin**, **kshell** 을 허가시켜야 합니다.
- **Telnet** – kerberos 화된 telnet 를 리용하려면 **krb5-telnet** 를 허가시켜야 합니다.
- FTP – FTP 접근을 제공하려면 **ftp** 의 root 로 가진 기본실체에 대한 열쇠를 작성하고 추출해야 합니다. FTP 봉사기의 완전자격주콤퓨터이름을 설정한 다음 **gssftp** 를 허가시켜야 합니다.
- IMAP – kerberos 화된 IMAP 봉사기를 리용하기 위해 **cyrus-sasl-gssapi** 패키지를 설치하면 **cyrus-imap** 패키지는 kerberos 5 를 리용합니다.

cyrus-sasl-gssapi 패키지는 GSS-API 인증을 지원하는 Cyrus SASL 삽입 프로그람들을 포함합니다. Cyrus IMAP 는 **cyrus** 사용자가 **/etc/krb5.keytab** 에서 정확한 열쇠를 찾을수 있고 기본실체의 root 가 **imap** 로 설정되여있다면 kerberos 와 정확히 동작합니다.

Cyrus-imap 를 대신할수 있는것으로서 **dovecot** 패키지가 있는데《붉은별》 봉사기용체계 3.0 에 포함되여있습니다. 이 패키지는 IMAP 봉사기를 포함하지만 현재까지 GSS-API 와 Kerberos 를 지원하지 않습니다.

CVS – kerberos 화된 CVS 봉사기를 리용하기 위해 **gserver** 는 **cvs** 를 root 로 가진 기본실체를 리용하며 그렇지 않은 경우에는 CVS **pserver** 와 동일합니다.

제10절. 보안쉘봉사기(SSH Server)

이 절에서는 ssh 의 개념과 openssh 봉사기를 리용하기 위한 openssh 봉사기 및 의뢰기설정, 매 사용자에 대한 openssh 설정, openssh 의뢰기도구의 리용방법에 대하여 설명합니다.

1. SSH 봉사기 개요

보안쉘봉사기(SSH Server)는《붉은별》 봉사기용체계 3.0 에서 SSH 규약을 실현하기 위한 공개원천쏘프트웨어이며 판본은 5.3p1 입니다.

1) 사용목적

보안쉘(Secure Shell: SSH)은 telnet, rlogin, Remote Shell (RSH)와 같은 안전하지 못한 원격가입과 지령실행도구들을 대신하는 망규약입니다. SSH 는 통화를 암호화하며 통화도청과 통과암호도난을 막습니다.

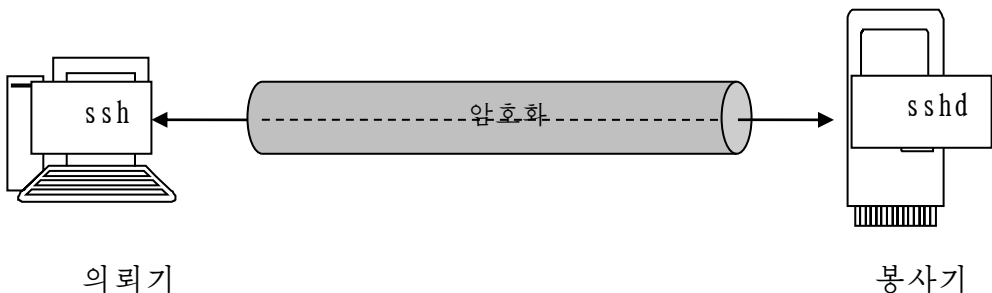



그림 27. SSH 에 의한 암호화

OpenSSH는 SSH를 지원하기 위한 공개원천쏘프트웨어이며 다음과 같은 특징을 가집니다.

- OpenSSH는 보호된 통로를 통하여 원격 TCP포구를 회송(forwarding) 할수 있는 능력을 포함합니다. 이것은 하나의 ssh접속을 통하여 추가적인 TCP접속들을 다중화하여 접속을 숨기고 안전치 못한 규약들을 암호화하는데 리용되며 방화벽을 우회하는데 리용됩니다. 원격주콤퓨터에 접속하기 위해 OpenSSH를 리용할 때 X Window System 통로가 자동적으로 만들어지며 http와 VNC와 같은 다른 규약들이 쉽게 회송될수 있습니다.
- 그외에 일부 3자쏘프트웨어는 SSH를 통한 암호화통로(tunnelling)를 지원합니다. 여기에는 DistCC, CVS, rsync, fetchmail이 있습니다. 일부 조작체계들에서 원격화일체계들은 sshfs (FUSE리용), shfs, lufs, podfuk와 같은 도구를 리용하여 SSH를 통하여 탑재될수 있습니다.
- OpenSSH를 리용하여 무선(ad hoc) SOCKS대리봉사기를 창조할수 있습니다. 이것은 보통의 포구회송으로 진행할수 있는것보다 더 유연한 대리봉사를 할수 있게 합니다.
- 4.3판본부터 OpenSSH는 OSI 층 2/3 tun에 기초한 VPN을 실현합니다. 이것은 OpenSSH의 가장 유연한 암호화능력이며 SOCKS를 리용하기 위한 변경을 진행함이 없이 원격 망자원들에 투명하게 접근할수 있게 합니다.

그밖의 특징들은 다음과 같습니다.

- 강력한 암호화(pilsung, 3DES, Blowfish)
- X11 forwarding-암호화된 방법으로 원격 X Window조종
- Port forwarding
- 강력한 인증(공개열쇠, 1회용통과암호, kerberos 인증)
- SSH2 규약지원
- kerberos와 AFS허가증통행
- 자료압축
- TCP Wrapper지원

2) 화일목록

OpenSSH 봉사기를 리용하려면 봉사기에 openssh 패키지들(openssh, openssh-server, openssh-clients)을 설치하여야 하며 의뢰기들에는 openssh, openssh-clients 패키지들을 설치하여야 합니다.

3) 쏘프트웨어의 구성관계

OpenSSH 는 일반 OpenSSH 패키지(openssh)와 OpenSSH 봉사기(openssh-server)와 의뢰기(openssh-clients)패키지로 나누어져있으며 기본쏘프트웨어인 ssh(의뢰기), sshd(봉사기), scp, sftp, sftp-server, ssh-config, sshd-config, 그리고 보조쏘프트웨어들인 ssh-keygen, ssh-keyscan, ssh-keysign, ssh-agent, ssh-add, ssh-rand-helper 쏘프트웨어로 구성되여있습니다.

4) 가동환경

ssh 봉사기쏘프트웨어는《붉은별》 봉사기용체계 3.0 이 동작하는 하드웨어 및 쏘프트웨어환경에서 동작합니다.

특별한 자원요구는 제기되지 않으며 망장치가 설치되여있으면 됩니다.

2. SSH 봉사기 설치

- 쏘프트웨어의 설치

  《붉은별》 봉사기용체계 3.0 에는 기정으로 ssh 쏘프트웨어가 설치되여있습니다. 즉 openssh-server-5.3p1, openssh-clients-5.3p1, openssh-5.3p1 패키지들이 기정적으로 설치됩니다.

  Ssh 봉사를 리용하려면 모든 의뢰기들에 openssh-clients-5.3p1, openssh-5.3p1 패키지를 설치하여야 합니다.

  ssh 봉사기에는 추가적으로 openssh-server-5.3p1 패키지를 설치하여야 합니다.

3. 보안쉘봉사기(SSH Server)의 작업절차

1) 봉사의 시작과 중지

- 봉사의 시작

  ssh 봉사기를 사용하기 위해서 먼저 ssh 봉사대몬을 시작합니다. 이때 봉사대몬은 기정으로 구성된 설정에 따라 동작합니다 (3.사용방법을 참고할것).

- 봉사의 중지

  ssh 봉사대몬(sshd)이 시작되여있는 경우 대몬중지지령(service servicename stop)으로 봉사대몬을 중지시킵니다.

2) OpenSSH 봉사기구성화일 설정

OpenSSH 는 아래와 같은 용도로 사용할수 있습니다.

- telnet 와 rlogin, rsh, rdist, rcp 쏘프트웨어의 대용쏘프트웨어
- 망을 통한 안전한 예비보관
- 원격명령문 실행
- 인터네트를 통해 공동의 정보에 접근할 때
- 안전한 방법으로 원격화일전송

OpenSSH 를 리용하려면 OpenSSH 의 몇가지 설정값을 변경하거나 확인해야 합니다. 변경해야 할 화일은 아래와 같습니다.

/etc/ssh/ssh_config(OpenSSH 의뢰기설정화일)
/etc/ssh/sshd_config(OpenSSH 봉사기설정화일)
/etc/pam.d/sshd(OpenSSHPAM 지원설정화일)
/etc/rc.d/init.dsshd(OpenSSH 초기화화일)
/etc/ssh/sshd_config:

sshd_config 화일은 OpenSSH 대몬의 동작조정설정값을 설정할수 있는 전반적인 체계설정화일입니다. 이 화일에는 한행에 한쌍씩 실마리어와 값이 정의되며 실마리어는 대소문자를 구분하지 않습니다.

여기에 있는것들은 ssh 의뢰기쏘프트웨어를 조작할 때 최상의 보안을 위해 설정해야 할 가장 중요한 실마리어입니다. 보다 상세한 특별설정사항목록을 얻으려면 sshd(8)의 안내페지를 참고해야 합니다. 기본값을 조작체계에 맞도록 변경합니다. 강조체로 된 문장은 설정화일의 내용중에서 필요에 맞도록 최적화하거나 조정해야 하는것들입니다.

/etc/ssh/sshd_config 로 sshd_config 화일을 요구에 맞게 편집합니다. 아래에 권고설정값들을 보여주었습니다.

이 설정은 ssh 의 체계전반에 대한 설정화일입니다.

```
Port 22
Listenaddress 207.35.78.3
Hstkey /etc/ssh/ssh_host_key
Hoostkey /etc/ssh/ssh_host_dsa_key
Hostkey /etc/ssh/ssh_host_rsa_key
Serverkeybits 768
Logingracetime 60
Keyregenerationinterval 3600
Permitrootlogin no
Ignorerhosts yes
Ignoreuserknownhosts yes
Strictmodes yes
Xl1forwarding no
Printmotd yes
Keepalive yes
```

Syslogfacility auth
Loglevel info
Rhostsauthentication no
Rhostsrsaauthentication no
Rsaauthentication yes
Passwordauthentication no
Permitemptypasswords no
Allowusers ohsungwon
Pamauthenticationviakbdinst yes
Subsystem sftp /usr/libexec/openssh/sftp-server

이 설정은 ssh_config 화일에 대해 다음의 특정한 값을 설정합니다.

Port 22

<port>설정값은 ssh 대몬이 접속요청을 받을 때 련결할 포구를 정의합니다. 기본포구는 22 번입니다.

ListenAddress 207.35.78.3

<ListenAddress>설정값은 ssh 봉사기의 소케트가 결합될 대면부망의 IP 주소를 정의합니다. 기본값은<0.0.0.0>입니다. 보안강화를 위해 가능한껏 주소를 제한해야 합니다. 요구되는 값으로만 제한할수 있습니다.

Hostkey /etc/ssh/ssh_host_key
Hostkey /etc/ssh/ssh_host_dsa_key
Hostkey /etc/ssh/ssh_host_rsa_key

이 설정값은 서로 다른 개별주콤퓨터열쇠의 위치를 나타냅니다.

ServerKeyBits 768

<ServerKeyBits>설정값은 봉사기열쇠에서 몇비트를 사용할것인가를 정의합니다. 이 비트는 대몬이 해당 rsa 열쇠를 생성하기 시작할 때 사용됩니다.

LoginGraceTime 60

<Logingracetime>설정값은 봉사기로 접속요청이 들어온 사용자가 접속을 하지 못했을 때 접속을 완료하기전까지 봉사기가 대기할 시간을 초단위로 정의합니다. 이 설정은 낮은 값을 설정하도록 합니다. 례를 들어 1024 개의 동시련결이 같은 시간에 이루어진다면 봉사기가 감당할수 없게 됩니다.

KeyRegenerationInterval 3600

<Keyregenerationinterval>설정값은 자동적으로 열쇠를 다시 생성하기전까지 봉사기가 대기할 시간을 초단위로 정의합니다. 이 설정값은 획득된 인자가 해득되는것을 방지하기 위한 보안기능입니다.

PermitRootLogin no

<PermitRootLogin>설정값은 ssh 를 리용하여 root 로 접속이 가능한가를 결정하는 설정값입니다. 이 설정값에 대해 <yes>를 선택하지 않도록 합니

다. 일반 ID 로 접속한 다음 su 를 리용하여 root 로 전환하는것이 훨씬 안전합니다.

IgnoreRHosts yes

<IgnoreRHosts>설정값은 인증시 rhosts 와 shosts 화일의 사용여부를 정의합니다. 보안상의 리유로 인증할 때 rhosts 와 shosts 화일을 사용하지 않도록 합니다.

IgnoreUserKnownHosts yes

<IgnoreUserKnownHosts>설정값은 ssh 대몬이 RhostsRSAAuthentication 과정에서 매 사용자의 $HOME/.ssh/known_hosts 를 무시할것인가 하는 여부를 정의합니다. Rhosts 화일을 허용하지 않았으므로 <yes>로 설정하는것이 안전합니다.

Strictmodes yes

<Strictmodes>설정값은 ssh 가 접속을 받기전 매 사용자의 home 등록부실행권한과 rhosts 화일의 검사여부를 결정합니다. 이 설정값은 항상 <yes>로 설정되여있어야 하는데 그것은 사용자들이 화일이나 등록부의 실행권한을 누구나 쓸수 있도록 설정하는 경우가 있기때문입니다.

X11Forwarding no

<X11Forwarding>설정값은 해당봉사기에서 x11 발송기능여부를 설정합니다. 《붉은별》 봉사기용체계 3.0 에서는 GUI 없이 봉사기를 설정하기때문에 안전을 위하여 이 설정은 <no>로 설정합니다.

PrintMotd yes

<PrintMotd>설정값은 사용자가 접속하는 경우 ssh 가 /etc/motd 화일의 내용을 보여줄것인가 하는 여부를 결정합니다. /etc/motd 화일은 《The message of the day(오늘의 통보문)》의 략자입니다.

SysLogFacility AUTH

<SysLogFacility>설정값은 sshd 가 접속통보문을 남길 때 사용할 facility 코드를 결정합니다. Facility 라는 통보문을 생성하는 아래준위체계를 의미하며 이 경우 <AUTH>로 설정합니다.

LogLevel INFO

<LogLevel>설정값은 sshd 로부터 접속통보문이 전달될 때 사용하는 준위를 정의합니다. INFO 는 권고되는 값입니다. 다른 설정가능한 설정값에 대해서는 안내페지를 참고하십시오.

RhostsAuthentication no

<RhostAuthentication>설정값은 sshd 가 rhosts 에 의한 인증을 사용할것인가를 정의합니다. Rhosts 인증은 안전하지 못하므로 이 설정값을 사용하지 않습니다.

RhostsRSAAuthentication no

<RhostsRSAAuthentication>설정값은 RSA 주콤퓨터인증과 맞추어 rhosts 인증의 사용여부를 정의합니다. 이 값은 <no>로 설정합니다.

RSAAuthentication yes

<RSAAuthentication>설정값은 RSA 인증의 시도여부를 정의합니다.이 설정값은 ssh1 규약에만 사용하기 위해 예약된것입니다. 만일 ssh1 을 사용하고 조작상 보다 안전하게 조작하려면 이 설정값을 <yes>로 설정해야 하는데 그 까닭은 이 설정값이 ssh2 규약에 대해서는 적용되지 않기때문입니다.(ssh2 는 RSA 대신 dsa 를 사용합니다). RSA 는 인증을 하기 위해 ssh-keygen 편의프로그람에 의해 생성된 공개열쇠와 비공개열쇠쌍을 사용합니다.

PasswordAuthentication no

<PasswordAuthentication>설정값은 인증할 때 암호화인증방법의 사용여부를 결정합니다. 강력한 보안을 위해 이 설정값은 항상 <no>로 설정해야 합니다. <PasswordAuthenticationno>를 sshd_config 화일에 두지 않으면 누군가가 암호를 추측하여 접근할수도 있습니다. <Passwordauthentication no>를 설정한 상태에서 콤퓨터에 공개열쇠를 두지 않으면 누구도 접근할수 없으며 이것이 이 설정값의 사용의도입니다. Windows 의뢰기쏘프트웨어인 putty 를 리용하려면 이 설정값을 <no>로 설정하면 안됩니다. 이렇게 하면 putty 로 봉사기에 접속할수 없습니다.

PermitEmptyPasswords no

<PermitEmptyPasswords>설정값은 우의 <PasswordAuthentication> 설정값과 밀접한 관련이 있으며 암호인증과정에서 암호가 입력되지 않은 등록자리에 대한 접속허용여부를 정의합니다. 봉사기에서 암호인증을 사용하지 않으므로 안전을 위하여 이 설정값은 <no>로 설정합니다.

AllowUsers admin

<Allowusers>설정값은 어떤 사용자가 ssh 에 접근할수 있는가를 정의하고 조종합니다. 여러 사용자를 공백으로 구분하여 설정할수 있습니다.

Ciphers pilsung128-cbc

<Ciphers>설정값은 규약판본 2 에서 우선권의 순서에 따라 허용되는 암호들을 지정합니다. 여러개의 암호들은 반점으로 구분합니다.

지원되는 암호들은 pilsung128-cbc, pilsung256-cbc, 3des-cbc, aes128-cbc, aes192-cbc, aes256-cbc, aes128-ctr, aes192-ctr, aes256-ctr, arcfour128, arcfour256, arcfour, blowfish-cbc, cast128-cbc 입니다. 기정값은 국가표준대칭암호화알고리듬인 pilsung 128-cbc 입니다.

3) 사용방법

국부체계에서 사용자는 SSH 의뢰기를 시작하여 sshd 대몬을 실행하는 원격봉사기에 접속합니다. 사용자가 성과적으로 인증되면 대화식의 접속이 시작되며

사용자는 원격체계에서 지령들을 실행할수 있습니다. SSH 는 지령해석기라는 의미에서 셸이 아니며 원격체계상의 셸을 리용할수 있습니다.

대화식의 가입외에 사용자는 기존의 통로를 통하여 TCP 망접속을 리용하여 X11 와 다른 망응용쏘프트웨어들을 리용할수 있으며 scp 와 sftp 도구들을 리용하여 화일들을 복사할수 있습니다. OpenSSH 는 인증, 권한부여, 계산자리관리, 대화관리에 PAM 흐레임워크를 리용하도록 구성됩니다. 통과암호유효기간의 끌내기와 잠그기는 적합한 PAM 기능들을 통하여 조종됩니다.

SSH 의뢰기와 SSH 봉사기사이의 통신은 SSH 규약판본 2.0 을 리용합니다. SSH 규약은 매 주콤퓨터가 주콤퓨터에 고유한 열쇠를 가질것을 요구합니다. SSH 의뢰기가 접속을 시작할 때 Diffe-Hellman 규약을 리용하여 열쇠들을 교환합니다. 대화열쇠를 생성하고 모든 통화는 이 대화열쇠와 합의된 알고리듬을 리용하여 암호화됩니다.

SSH 가 지원하는 기정암호화알고리듬들은 pilsung(국가표준대칭암호화) 입니다. 이 기정값은 봉사기구성화일에서 《ciphers》예약어로써 재정의할수 있습니다.

SSH 가 지원하는 기정의 통보문인증코드알고리듬은 SHA-1 와 MD5 입니다. 이 기정값은 봉사기구성화일에서 예약어 MACs 를 리용하여 재정의할수 있습니다.

암호화는 별도의 쏘프트웨어패키지인 OpenSSL 패키지 에 의해서 제공됩니다. 아래에 암호화, 완전성검사, 인증서형식, 열쇠교환알고리듬에 관한 기정 SSH 설정을 설명합니다.

- 암호화: SSH 가 리용하는 기정암호는 pilsung128-cbc(CBC 방식의《필승) 암호》입니다.
- 완전성검사: 자료완전성은 매 파케트에 공유비밀, 파케트차례번호, 파케트의 내용으로부터 계산된 통보문인증코드(MAC)를 포함함으로써 보호됩니다. 통보문인증알고리듬과 열쇠는 열쇠교환과정에 협상합니다. 초기에 MAC 는 효과가 없으며 그의 길이는 령이여야 합니다. 열쇠를 교환한 다음 암호화를 진행하기전에 파케트자료의 련결로부터 선택한 MAC 를 계산합니다.

mac = MAC(key, sequence_number || unencrypted_packet)

여기서 unencrypted_packet 는 MAC(길이마당, 자료부와 채우개)가 없는 전체파케트이고 sequence_number 는 uint32 로 표현되는 암시적인 파케트차례번호입니다. 차례번호는 첫 파케트에 대하여 령으로 초기화되며 매 파케트마다 암호화나 MAC 가 리용되고있는가에 관계없이 증가합니다. 이것은 열쇠나 알고리듬들이 후에 재협상된다고 해도 절대로 재설정되지 않으며 매 2^32 파케트 후에 령으로 됩니다. 파케트차례번호 그자체는 전송파케트에 포함되지 않습니다.

MAC 알고리듬들은 매 방향에 대하여 따로 따로 실행되여야 하며 알고리듬들도 따로따로 선택해야 합니다. MAC 알고리듬으로부터 생기는 MAC 바이트들은 파케트의 마지막부분으로서 암호화없이 전송해야 합니다. MAC 바이트수는 선택된 알고리듬에 관계됩니다. 기정으로 정의된 MAC 알고리듬은 hmac-sha1(digest 길이=열쇠길이= 20)입니다.

- 인증서형식: 기정으로 리용하는 인증서형식은 Simple DSS 로 서명한 ssh-dss 입니다. 이 열쇠형식을 리용하는 서명과 검증은 SHA-1 해쉬를 리용하는 DSS(Digital Signature Standard)에 따라 진행됩니다.
- 열쇠교환규약: 기정의 열쇠교환규약은 diffie-hellman-group1-sha1 입니다. diffie-hellman-group1-sha1 방법은 HASH 로서 SHA-1 을 가진 diffie-hellman 열쇠교환을 지정합니다.

4) OpenSSH 의뢰기설정

/etc/ssh/ssh_config 화일은 OpenSSH 의뢰기쏘프트웨어의 동작설정값을 설정할 수 있는 체계전반에 대한 설정화일입니다.

이 화일에는 한행에 한쌍씩의 실마리어와 값이 정의되며 실마리어는 대소문자를 구분하지 않습니다. 여기에 있는것은 ssh 의뢰기쏘프트웨어를 조작할 때 최상의 보안을 위해 설정해야 할 가장 중요한 실마리어입니다. 보다 상세한 특별설정사항목록을 보려면 ssh(1)의 안내페지를 참고해야 합니다. 기본값을 사용자의 요구와 조작체계에 맞도록 변경합니다. 강조체로 된 문장은 설정화일의 내용중에서 필요에 맞도록 최적화하거나 조정해야 하는것입니다.

vi /etc/ssh/ssh_config 로 ssh_config 화일을 필요에 맞게 편집합니다.

아래는 권고설정값입니다.

```
#다양한 설정값에 대해서 대부분 적용되는 설정
Host*
Forwardagent no
Forwardxl1 no
Rhostauthentication no
Rhostsrsaauthentication no
Rsaauthentication yes
Passwordauthentication no
Fallbacktorsh no
Usersh no
Batchmode no
Checkhostip yes
Stricthostkeychecking yes
Identityfile ~/.ssh/identity
Identityfile ~/.ssh/id_dsa
```

Identityfile ~/.ssh/id_rsa
Port 22
Protocol 2,1
Cipher pilsung128-cbc
Escapechar ~
이 설정은 ssh_config 화일에 대해 다음의 특정한 값을 설정합니다.

Host*
<Host>설정값은 설정화일에서 이후의 모든 선언문과 설정값들이 host 실마리어 다음에 설정된 류형들중 하나에 맞는 주콤퓨터로 제한합니다. *류형은 다음번 host 실마리어가 나오기까지 모든 주콤퓨터에 대해 적용한다는 의미입니다.
이 설정값으로 하나의 ssh_config 화일에서 다른 주콤퓨터에 대해 각각 다른값을 선언할수 있습니다. 특히 사용자암호를 입력하지 않고 ssh 를 리용하여 망을 통해 자동예비보관을 하려고 할 때 필요합니다. 이렇게 함으로써 이런 의미로 사용할 부분을 미리 설정할수 있고 특정한 주콤퓨터의 암호를 묻는 기능을 중지시키게 할수 있습니다.

ForwardAgent no
<forwardagent>설정값은 접속대리자가 있을 때 어떤것이 원격봉사기로 발송되여야 하는가를 정의합니다.

Forwardx11 no
<Forwards11>설정값은 X-Windows 의 GUI 환경을 사용하는 사람이 원격봉사기에서 자동적으로 X11 작업을 통해서 재목록화하는 경우에 사용합니다.
여기서 설정한 봉사기는 GUI 가 설치되지 않았으므로 안전을 위해 이 설정을 no 로 합니다.

RhostsAuthentication no
<Rhostsauthentication>설정값은 rhosts 에 의한 인증의 사용여부를 정의합니다. Rhosts 인증은 보안상 좋지 않기때문에 이 설정값을 사용하지 않습니다.

RhostsRSAAuthentication no
Rhostsrsaauthentication 설정값은 RSA 주콤퓨터인증과 맞추어 rhosts 인증의 사용여부를 정의합니다. 이 값은 no 로 설정합니다.

RSAAuthentication yes
<Rsaauthentication>설정값은 RSA 인증의 사용여부를 정의합니다. 이 설정값은 ssh1 규약에만 사용하기 위해 예약된것입니다. 만일 ssh1 만을 사용하여 보다 안전하게 조작하려면 이 설정값을 <yes>로 설정해야 하는데 그 리유는 이 설정값이 ssh2 규약에 대해서는 적용되지 않기때문입니다(ssh2 는 RSA 대신 DSA 를 사용합니다). RSA 는 인증을 하기 위하여 ssh-keygen 편의프로그람에 의해 생성된 공개열쇠 및 비공개열쇠쌍을 사용합니다.

PasswordAuthentication no

<PasswordAuthentication>설정값은 인증을 할 때 암호에 기초한 인증방법의 사용여부를 정합니다. 강력한 보안을 위해 이 설정값은 항상 no로 설정해야 합니다.

<PasswordAuthenticationno>을 sshd_config 화일에 넣어둡니다. 그렇지 않으면 누군가 암호를 추측하여 접근할수도 있습니다.

<Passwordauthenticationno>를 설정한 상태에서는 콤퓨터에 공개열쇠를 두지 않으면 누구도 접근할수 없으며 이것이 여기서 목적하는것입니다.

Windows의 리기쏘프트웨어인 putty를 리용하면 이 설정값을 <no>로 설정해서는 안됩니다. 그렇지 않으면 putty를 사용하여 봉사기에 접속할수 없습니다.

FallBackToRsh no

<Fallbacktorsh>설정값은 ssh 대몬을 리용한 련결이 실패한 경우 자동적으로 rsh를 사용할것인가의 여부를 결정합니다. Rsh 봉사는 안전하지 못하므로 이 설정값은 항상 <no>로 설정합니다.

UseRsh no

<UseRsh>설정값은 rlogin/rsh 봉사가 이 주콤퓨터에서 사용되는가에 대한 여부를 결정합니다. <fallbacktorsh>처럼 확실하게 <no>로 설정합니다.

BatchMode no

<BatchMode>설정값은 봉사기로 련결할 때 사용자명과 암호를 문의할것인지 여부를 결정합니다. 이 설정값은 스크립트를 생성하고 사용하여 암호의 입력을 요구하지 않을 때 쓸모있습니다(례를 들어 망을 통한 예비보관을 하기 위하여 scp 명령을 사용하는 스크립트같은 경우).

CheckHostIP yes

<checkhost>설정값은 DNS 속임을 추적하기 위하여 ssh가 주콤퓨터의 IP 주소를 추가로 검사할것인가의 여부를 정의합니다. 이 설정값은 <yes>로 선택할것을 권고하지만 속도가 떠지는 결함이 있습니다.

StrictHostKeyChecking yes

<Stricthostkeychecking> 설정값은 ssh가 $HOME/.ssh/known_hosts 화일에 자동적으로 새로운 주콤퓨터열쇠를 추가할것인가의 여부와 주콤퓨터열쇠를 주콤퓨터화일에 추가하지 않을것인가의 여부를 결정합니다. 이 설정값을 <yes>로 설정하면 트로이목마공격에 대해서 최대한의 보안을 실현할수 있습니다.

처음 시작할 때 이 설정값으로 <no>를 설정하면 ssh가 련결하려는 모든 일반주콤퓨터를 host 화일에 자동적으로 추가하고 이후 이 값을 yes로 설정하면 이 기능을 계속 리용할수 있습니다.

IdentityFile ~/.ssh/identity
IdentityFile ~/.ssh/id_dsa
IdentityFile ~/.ssh/id_rsa

이 설정값은 참고할수 있는 여러 인증증명화일을 설정합니다.

Port 22

Port 설정값은 ssh 가 원격주콤퓨터에 련결한 포구를 정의하며 기본포구는 22 번입니다.

Protocol 2,1

<protocol>설정값은 ssh 가 우선적으로 지원하는 규약판본을 정의합니다.

설정화일에서 기본설정값은 <2,1>입니다. 이것은 ssh 가 먼저 판본 2 로 시도한 다음 실패하는 경우 판본 1 로 접속한다는 의미입니다. 《붉은별》 봉사기용체계 3.0 에서는 보안상 리유로부터 이 설정값을 1 로 정의해도 판본 1 을 지원하지 않습니다.

Cipher pilsung128-cbc

<Cipher>설정값은 암호화과정에서 어떤 암호를 사용할것인가를 정의합니다.

기정으로 국가표준대칭암호화인 pilsung 암호를 사용하며 열쇠길이는 128, 256bit 를 사용할수 있습니다.

EscapChar ～

<EscapeChar>설정값은 련결을 완료할 때 사용하는 문자입니다.

/etc/pam.d/sshd:OpenSSHPAM 지원의 설정

보안이 보다 강화된 OpenSSH 를 위해서 OpenSSH 에서 PAM 암호인증기능을 사용할수 있도록 설정합니다. 이것을 위해서 /etc/pam.d/sshd 화일을 생성한 다음 아래의 내용을 추가합니다.

#touch /etc/pam.d/sshd 로 sshd 화일을 생성한 다음 아래의 내용을 추가합니다.

```
#%pam-1.0
authrequired/lib/security/pam_stack.soservice=system-auth
authrequired/lib/security/pam_nologin.so
accountrequired/lib/security/pam_stack.soservice=system-auth
accountrequired/lib/security/pam_access.so
accountrequired/lib/security/pam_time.so
passwordrequired/lib/security/pam_stack.soservice=system-auth
sessionrequired/lib/security/pam_stack.soservice=system-auth
sessionrequired/lib/security/pam_limits.so
sessionrequired/lib/security/pam_console.so
```

5) 매 사용자에 대한 OpenSSH 설정

의도한대로 설정이 끝나고 sshd 대몬이 동작하기 시작하면 사용자들이 도청의 위험성이 없는 련결을 할수 있도록 여기에 대한 새로운 공개 및 비공개열쇠를 생성합니다. sshd(8)안내페지에 있는 내용을 보면 다음과 같습니다.

비공개열쇠를 사용하여 암호화 및 복호화되는 암호화체계에서는 암호화열쇠로부터 해득열쇠를 빼내는것이 불가능합니다. 이것은 매 사용자는 공개 및 비공개열쇠쌍을 인증목적으로 생성한다는것과 관련됩니다. 봉사기는 공개열쇠를 알고 비공개열쇠는 오직 사용자만이 아는것입니다.

SSH2 에 사용되는 $HOME/.ssh/authorized_keys 화일과 SSH1 에 사용되는 $HOME/.ssh/authorized_keys 화일에는 접속이 허용된 공개열쇠목록이 있습니다. 사용자가 접속하면 ssh 쏘프트웨어는 봉사기와 통신하면서 인증에 사용할 열쇠쌍을 확인합니다. 봉사기는 이 열쇠의 허용여부를 검사하고 허용된것이면 사용자에게 (실제로 ssh 쏘프트웨어는 사용자를 대신하여 동작합니다) 사용자의 공개열쇠로 암호화된 란수를 보내는데 이 란수는 오직 적절한 비공개열쇠를 통해서만 해득할수 있습니다. 의뢰기쏘프트웨어는 봉사기에 드러내지 않으면서 비공개열쇠를 알게 되고 이 비공개열쇠를 리용하여 이 란수를 해득합니다.

1 단계

아래에서는 한명의 사용자에 대하여 새로운 SSH 비공개열쇠와 공개열쇠를 생성하는 방법을 설명합니다. 이 실례에서는 《붉은별》3.0(사용자용체계)와 《붉은별》 봉사기용체계 3.0 사이에 안전한 암호화련결이 이루어졌다고 가정합니다.

* 국부환경의 SSH2 를 위한 DSA 비공개열쇠와 공개열쇠를 생성하려면 아래와 같이 입력합니다.

```
[root@deep/]#su ohsungwon
[ohsungwon@deep/]$ssh-keygen -d
Generating DSA parameter and key.
Enter file in which to save the key(/home/ohsungwon/.ssh/id_dsa):
Created directory '/home/ohsungwon/.ssh'.
Enter passphrase(empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in/home/ohsungwon/.ssh/id_dsa.
Your publickey has been saved in/home/ohsungwon/.ssh/id_dsa.pub.
The key fingerprint is:
 1f:af'aa:22:0a:21:85:3c:07:7a:5c:ae:c2:d3:56:64ohsungwon@deep
```

우의 실례에서는 SSH2 규약을 위한 일반적인 DSA 비밀열쇠와 공개열쇠를 생성하다고 가정합니다. SSH 규약 1 을 위한 RSA 비밀열쇠와 공개열쇠를 생성하려면 다음과 같이 열쇠를 생성할 때 <-d>설정값을 제거합니다.

[root@deep/]#su ohsungwon

[ohsungwon@deep/]$>ssh-keygen <-d>설정값을 제거하면 SSH2 규약대신에 SSH1 규약의 비밀열쇠 및 공개열쇠를 생성합니다.

SSH1 비밀열쇠는 identity, 공개열쇠는 identity.pub 로 됩니다.

만일 여러개의 등록자리를 가지고있다면 매 등록자리에 대하여 서로 다른 열쇠를 생성하려고 합니다. 이에 대해서 다음과 같은 독립적인 열쇠를 가질수 있습니다.

* 봉사기(1)
* 봉사기(2)

* 봉사기(3)

이 봉사기들은 매 봉사기들사이의 접근제한을 허용합니다. 례를 들면 봉사기(1)의 등록자리로 봉사기(2)의 등록자리나 봉사기(3)에 접근하는것을 금지할수 있습니다. 이 기능은 만일 어떠한 리유로 인증열쇠가 손상되였을 때 전체적인 보안을 강화합니다.

2 단계

SSH2 의 국부공개열쇠 id_dsa.pub 또는 SSH1 의 국부공개열쇠 identity.pub 를 /home/ohsungwon/.ssh 등록부에서 원격으로 복사하여 ssh2 의경우 authorized_keys2 로 ssh1 의 경우 authorized_keys 로 정의합니다. 화일을 복사하는 한가지 방법은 ftp 를 리용하여 화일을 복사하는것이고 또 다른 한가지 방법은 체계관리자에게 발송하는 우편에 공개열쇠를 통보문으로 발송하는것입니다. 다만 ~/.ssh/id_dsa.pub 또는 ~/.ssh/identity.pub 화일의 내용을 통보문에 넣기만 하면 됩니다.

그 단계를 차례대로 보면 다음과 같습니다.

- 사용자는 ssh-keygen 을 실행하여 DSA 또는 RSA 열쇠쌍을 생성합니다.

이것은 $HOME/.ssh/id_dsa(SSH2) 또는 $HOME/.ssh/identity(SSH1)의 비공개열쇠와 $HOME/.ssh/id_dsa.pub(SSH2) 또는 $HOME/.ssh/identity.pub(SSH1)의 공개열쇠를 국부봉사기의 사용자의 등록부에 보관합니다.

- 사용자는 id_dsa.pub 열쇠(SSH2) 또는 identity.pub 열쇠(SSH1)화일을 원격봉사기에 있는 사용자등록부로 복사하여 SSH2 는 $HOME/.ssh/authorized_keys2,SSH1 는 $HOME/.ssh/authorized_keys(SSH1)로 복사합니다.(authorized_keys2 또는 authorized_keys 화일은 전통적인 $HOME/.rhosts 화일에 해당하며 한행을 매우 길게 작성할수는 있지만 하나의 열쇠는 한행에 정의해야 합니다).

봉사기 1 봉사기 2
사용자:ohsungwon 사용자:ohsungwon
암호문:qwerty1
암호문:qwerty2
비공개열쇠:id_dsa
비공개열쇠:id_dsa
공개열쇠:id_dsa.pub authorized_keys2
authorized_keys2 공개열쇠:id_dsa.pub

봉사기(2)에 대해서도 같은 방법을 수행합니다. 봉사기(2)에 있는 ohsungwon 이라는 사용자의 공개열쇠는 첫번째 봉사기(1)에 있는 ohsungwon 이라는 사용자의 $HOME 등록부로 보내여 authorized_key2 라는 화일로 보관합니다.

OpenSSH 의 공개열쇠는 한행의 문자렬입니다.

암호의 변경

ssh_keygen 에서 -p 설정값을 리용하면 언제든지 암호를 변경할수 있습니다.
암호를 변경하려면 다음과 같이 합니다.

[root@deep/]#su ohsungwon
[ohsungwon@deep/]$ssh-keygen –d -p
Enter file in which the key is(/home/ohsungwon/.ssh/id-dea):
Enter old passphrase:
 Key **has** comment‘dsaw/ocomment’
Enter new passphrase(emptyfornopassphrase):
Enter same passphrase again:
Your identification has been saved with the new passphrase.

SSHl 규약의 동작중 사용자암호를 변경하려면 우의 실례에서 -d 설정값을 제거하고 실행합니다.

6) OpenSSH 의뢰기 도구

아래에 보여준 명령문은 일반적으로 사용하는 명령문의 일부입니다.
그러나 실제로는 훨씬 많으므로 OpenSSH 에 대해서 보다 상세한 정보와 설명을 보려면 안내페지를 참고하십시오.

① SSH

ssh(SecureShell)명령은 안전하지 않은 망사이에서 암호화된 통신을 제공합니다. 이것은 원격봉사기로 안전하게 접속하여 원격봉사기에서 명령을 실행시키는 쏘프트웨어입니다. ssh 는 telnet 이나 rlogin, rcp, rdist, rsh 와 같이 안전하지 못한 쏘프트웨어에 대한 좋은 대책안으로 되는 쏘프트웨어입니다.
원격봉사기에 접속하기 위한 명령은 아래와 같습니다.

[root@deep/]#ssh –l <login_name> <hostname>
실례:
[root@deep/]#ssh –l ohsungwon deep.openna.com
ohsungwon@deep.openna.com’s password:
LastLogin:Tue Oct 19 1999 18:13:00-0400 from deep.openna.com
No mail.
[ohsungwon@deep ohsungwon]$

우의 명령에서 <login_name>은 원격봉사기에 접근하기 위해서 사용하는 이름이며 <hostname>은 ssh 봉사기의 원격주소(IP 주소를 사용할수도 있습니다)입니다.

② SCP

scp(SecureCopy)편의프로그람은 국부환경체계에서 원격봉사기 또는 원격봉사기에서 국부봉사기로 화일을 복사할 때 사용하는 편의프로그람로서 scp명령을 리용하면 원격봉사기사이에서도 화일을 복사할수 있습니다.

-원격봉사기에서 국부봉사기로 화일을 복사하려면 다음의 명령을 리용합니다.

[root@**deep**/]#su ohsungwon
[ohsungwon@deep/]$scp –p <login_name@hostname>:/dir/for/file localdir/to/filelocation

실례:

[ohsungwon@deep/]$scp –p ohsungwon@mail:/etc/test1 /tmp
Enter passphrase for RSAkey‘ohsungwon@mail,openna.com’:
Test1 1 2KB 12.0KB/s 1 ETA:00:00:001 100%

-국부봉사기에서 원격환경봉사기로 화일을 복사하려면 아래와 같이 합니다.

[root@deep/]#su ohsungwon
[ohsungwon@deep/]$scp –p localdir/to/filelocation <username@hostname>:/dir/for/file

실례:

[**ohsungwon** @deep/]$scp -p /usr/bin/test2 ohsungwon@mail:/var/tmp
ohsungwon’s password:
test2 1 7KB 17.9KB/s 1 ETA:00:00:001 100%

<-p>설정값은 화일을 복사할 때 원천화일의 변경 및 접근시간과 방식을 보존해야 하는 경우에 이것을 지시하는 설정값입니다.

제11절.망화일체계봉사기(NFS Server)

이 절에서는《붉은별》 봉사기용체계 3.0에서 망화일체계봉사기(NFS Server)를 설치하고 리용하는 방법을 설명합니다.

여기서는 망화일체계봉사기(NFS Server)를 시작하고 중지하며 봉사내용을 설정하고 변경 하는 방법에 대하여 설명합니다.

또한 nfs봉사중에 nfs봉사내용을 변경하기 위한 exportfs편의프로그람과 그 리용방법에 대하여 설명합니다.

1. 망화일체계봉사기의 개요

망화일체계봉사기(NFS Server)쏘프트웨어는 화일체계공유와 봉사기의 자원공유를 목적으로 합니다.

망이 련결된 곳에서 화일체계공유와 부하분산을 위한 도구로 사용될수 있습니다.

망화일체계봉사기(NFS Server)가 아직까지는 Windows 화일체계와는 련동이 어려운 반면에 SAMBA는 Windows화일체계와도 련동합니다. 하지만 보안적인 측면과 성능적인 측면을 고려하여 NFS를 사용하는것이 더 효과적입니다. 즉 화일체계공유목적외에 봉사기무리를 형성하여 부하분산이나 여벌복사봉사 및 자료저장소봉사를 구축하는것이 목적이라면 NFS를 사용하는것이 좋습니다. NFS는 처음부터 UNIX계렬의 조작체계를 위한 화일체계공유를 위해 개발되였다면 SAMBA는 UNIX계렬의 조작체계와 Windows계렬의 조작체계간의 화일공유를 위해 개발되였다고 할수 있습니다. 또한 NFS는 디스크없이 단지 망으로 화일을 공유하여 NFS봉사기의 디스크를 NFS말단이 마치 자기자신의 디스크인것처럼 사용할수 있습니다.

용어해설

NFS: 망화일체계(Network File System)

화일체계공유의 봉사기자원공유를 목적으로 1980년대 후반기에 SUN사에서 NIS(망정보봉사,Network Information Service)와 함께 개발한 규약.

RPC: 원격수속호출(Remote Procedure Call)

쏘프트웨어들사이의 통신방식의 한가지입니다. 쏘프트웨어안의 일부 수속들을 망안의 다른 콤퓨터에 맡기는 방식을 가리킵니다. 실행결과는 보통의 수속호출과 같이 되돌림값으로서 넘겨 줍니다. 분산콤퓨터환경의 기본으로 되는 기술입니다.

2. 패키지의 설치와 해제

1) 설치패키지목록

기본패키지명: nfs-utils-1.2.2-7.RSS.i686

nfs봉사기는 rpc(원격수속호출 Remote Procedure Call)기반에서 동작하기때문에 동작하려면 portmap대몬이 시작되여있어야 하는데 이 대몬은 portmap패키지에 있습니다.

2) 패키지의 구성관계

- rpc.nfsd대몬

  이 대몬은 NFS대몬으로서 실제로 NFS로 련결된 화일체계의 공유를 실현해주는 대몬입니다.

- rpc.mountd대몬

이 대몬은 RPC(Remote Procedure Call, 원격수속호출)기반하에서 NFS 사용을 위한 적재를 가능하게 하는 대몬입니다.

- -portmap 대몬
  NFS 가 원래 RPC 기반하에서 동작하기때문에 필요한 대몬입니다.
  이 외에 중요한 /etc/exports 설정화일이 있습니다.
  이 쏘프트웨어는 《붉은별》 봉사기용체계 3.0 에서 동작합니다.

3) 망화일체계봉사기의 설치 및 해제

NFS 봉사기는 우리 식 조작체계《붉은별》 봉사기용체계 3.0 이 설치될 때 자동적으로 설치됩니다.

NFS 봉사기를 수동적으로 설치하는 경우에는 먼저 nfs-utils-1.2.2-4.el6.i686.rpm 패키지가 설치되여있는가를 반드시 확인하여야 합니다.

#rpm –qa | grep nfs

nfs-utils-1.2.2-4

우와 같은 결과가 나오지 않으면 이 패키지들이 설치되지 않은것이므로 설치하여야 합니다.

CD 를 리용하여 설치를 진행하는 경우에는 먼저 CD 구동기에《붉은별》 봉사기용체계 3.0 CD 를 넣고 탑재를 시켜야 합니다.

mount /dev/cdrom /mnt/cdrom

패키지들이 들어있는 등록부에서 설치하려는 패키지들이 있는가를 확인합니다. 확인이 끝나면 설치를 시작합니다.

rpm –ivh nfs-utils-1.2.2-4.el6.i686.rpm

NFS 를 해제하려면 지령행에서 다음과 같은 지령을 실행시켜야 합니다.

#rpm –e nfs-utils

3. 망화일체계봉사기 작업절차

/etc/export 화일을 편집하여 봉사내용을 설정하며 조작탁에서 지령을 실행하여 봉사를 시작하고 중지합니다.

NFS 를 리용하려면 봉사기와 의뢰기에 동시에 portmap 대몬이 실행되여있어야 합니다.

- NFS 봉사의 시작, 중지, 재시작, 상태확인
  - 봉사의 시작
    조종탁에서 다음의 지령을 실행합니다.
    #service nfs start

- 봉사의 중지
  #service nfs stop

- 봉사의 재시작
  #service nfs restart

- 봉사의 상태확인
  # service nfs status

– NFS 관련 대몬들의 실행점검

NFS 대몬들이 정상적으로 실행이 되였는가를 확인해보는 방법에 대해서 설명합니다. rpcinfo 라는 지령을 리용하면 NFS 봉사기에 필요한 대몬들(rpc.mountd, rpc.nfsd)이 정상적으로 실행이 되고있는가를 확인할수 있습니다.

rpcinfo –p
rpcinfo –p 172.29.88.200

– /etc/exports 화일

이 화일은 NFS 설정화일로서 적재를 허용할 위치와 NFS 적재추가선택 항목을 설정하기 위한 화일입니다.

설정형식: [적재할 등록부] [허용할 NFS 의뢰기](설정추가선택항목들)

실례:

/web_data 172.29.88.32(rw)

이 설정은 172.29.88.32 라는 의뢰기에서 NFS 봉사기에 존재하는 /web_data 로의 적재를 허용한다는 뜻입니다. 추가선택항목의 rw 는 NFS 의뢰기에서 읽기쓰기가능하다는 뜻입니다.

/data 172.29.88.32(ro)

이 설정은 NFS 봉사기의 /data 라는 등록부에 NFS 의뢰기에서의 적재를 허용하며 읽기만 할수 있다는 뜻입니다.

/var/log   172.29.88.32(rw,root_squash)

NFS 봉사기와 NFS 의뢰기의 root 에 대한 보안조치입니다. NFS 의뢰기에서 NFS 봉사기로 root 권한으로 적재할 경우에 NFS 봉사기에서 root 권한을 부여하는 것이 아니라 nfsnobody 권한을 부여하게 된다는 뜻입니다. 만일 NFS 의뢰기에서 NFS 봉사기의 적재시에 root 를 일치시키려고 한다면 no_root_squash 라는 추가선택항목을 사용하면 됩니다. 즉 root 에 있어서는 추가선택항목이 지정되지 않을 경우의 기본값은 root_squash 가 됩니다.

/var/log   172.29.88.32(rw,no_root_squash)

이 추가선택항목의 no_root_squash 항목에 이해 NFS 의뢰기의 root 는 NFS 의 봉사기로 적재를 했을 경우에 NFS 봉사기에서의 root 사용자와 일치되게 됩니다. 하지만 가능한 이 설정은 보안을 위해서 사용하지 않는것이 좋습니다.

/home 172.29.88.32(rw,all_squash)

root 사용자와는 반대로 일반사용자의 경우에는 no_all_squash 가 기본값이 됩니다. 즉 NFS 의뢰기에서 NFS 봉사기로 적재할 경우에 동일사용자가 존재한다면 root 를 제외한 일반사용자는 동일한 사용자로 권한을 줍니다. 즉 동일한 사용자가 존재할 경우에는 그 사용자의 권한으로 NFS 봉사기에서도 사용할수 있다는 뜻입니다. 즉 일반사용자의 경우에는 no_all_squash 가 기본값이 됩니다. 실례의 경우에는 all_squash 를 사용했으므로 일반사용자의 경우에도 모두 nfsnobody 로 권한을 주게 됩니다. 만약 동일한 사용자로 되게 사용하려면 추가선택항목을 지정하지 않거나 no_all_squash 라는 항목을 지정하면 됩니다.

- exportfs 쏘프트웨어

exportfs 쏘프트웨어는 nfs 봉사자료를 변경하기위한 편의프로그람입니다.

exportfs –o 주콤퓨터명 1:경로 1 주콤퓨터명 2:경로 2…
봉사자료추가

exportfs –a
모든 정적봉사자료봉사

exportfs –i
정적봉사자료무시

exportfs –r
봉사내용을 정적봉사내용으로 복귀

exportfs –u 주콤퓨터명 1:경로 주콤퓨터명 2:경로…
봉사등록부해제

exportfs –f
봉사등록부초기화

구체적인 내용을 알려면 exportfs 의 안내페지를 참고하십시오.

제12절. 망시간규약봉사기(NTP Server)

이 절에서는《붉은별》 봉사기용체계 3.0 에서 망시간규약봉사기(NTP Server)의 사용방법을 설명합니다.

1. 망시간규약봉사기(NTP Server) 설치

망시간규약봉사기(NTP Server)는 우리 식 조작체계《붉은별》 봉사기용체계 3.0 에서 봉사기와 의뢰기와의 시간동기화를 실현하기 위한 봉사대몬입니다.

망시간봉사기가 설정되고 의뢰기들이 봉사기와의 시간동기화를 설정하면 의뢰기는 봉사기의 시간과 동기화되여 봉사기의 체계시간이 의뢰기의 체계시간으로 됩니다.

- 화일목록

Ntp-4.2.4p8-02.i686.rpm

- 화일설치

망시간규약봉사기(NTP Server)의 설치는 우리 식 조작체계《붉은별》 봉사기용체계 3.0 의 쏘프트웨어설치방식에 따릅니다.

개별적 쏘프트웨어를 설치하려는 경우 지령입력창에서 아래의 명령으로 설치합니다.

#rpm –ivh ntp-4.2.4p8-02.i686.rpm

2. 망시간규약봉사기의 작업절차

- 봉사의 시작

ntp.conf 는 기정값을 그대로 리용합니다. 다만 봉사기주소항목들을 비활성화해야 합니다. 이 주소들은 ntpd 가 동작하는 봉사기가 시간봉사기로 되는 경우 필요없는 항목들이며 시간봉사기가 따로 있는 경우에만 유효합니다. 비활성화는 행의 첫 머리부에 문자 #를 붙입니다.

ntp.conf 화일은 /etc 등록부에 있습니다.

ntpd 의 시작, 재시작은 일반대몬과 같은 방식으로 진행합니다.

지령입력창에서 아래의 지령을 실행하여 대몬을 시작합니다.

#service ntpd start

ntpd 가 실행되면 아래의 통보문이 현시됩니다.

ntpd 봉사를 시작합니다: [확인]

- 봉사의 재시작

지령입력창에서 다음의 지령을 실행하여 봉사를 재시작합니다.

#service ntpd restart

- 봉사의 중지

봉사의 중지는 다음의 명령으로 진행합니다.

#service ntpd stop

– 봉사의 상태확인

봉사의 상태확인은 다음의 명령으로 진행합니다.

```
#service ntpd status
```

3. 망시간규약봉사기의 사용방법

ntp 봉사기를 리용한 의뢰기의 시간동기화설정에 대하여 설명합니다.

- 시간설정창문을 열고 <시간대>표쪽에서 시간대를 <평양>으로 설정합니다.

-<인터네트시간>태브에서 자동동기화단추를 선택한 다음 본문창문에 시간봉사기의 령역주소를 입력하고 <갱신>단추를 누릅니다.

제13절. 모뎀인증봉사기(Radius Server)

이 절에서는《붉은별》 봉사기용체계 3.0 에서 FreeRADIUS 봉사기의 일반설정과 구성 및 보안설정, 그것을 리용하는 방법을 설명합니다.

1. 모뎀인증봉사기의 개요

원격인증전화접속사용자봉사(RADIUS:Remote Authentication Dial In User Service)는 모뎀을 통하여 망에 접속하려는 사용자들의 계산자리를 관리하는 인증중심의 망봉사입니다.

《붉은별》 봉사기용체계 3.0 에 포함된 Radius 봉사기는 모뎀으로 망에 접속하려는 사용자들의 인증을 관리하는 쏘프트웨어로서 판본은 2.1.9 입니다.

FreeRADIUS 는 RADIUS 규약을 리행하는 인터네트인증대몬으로서 RFC2865 에 정의되여있습니다. 그것은 모뎀사용자에 대한 인증을 진행하게 하는 망접근봉사기(NAS)를 허가합니다.

또한 RADIUS 의뢰기는 Web 봉사기, 방화벽, Unix 사용자가입 등 기타 여러가지에 리용될수 있습니다. RADIUS 의 리용은 새로운 사용자를 추가하거나 삭제할 때 진행하는 모든 재구성작업량을 최소화하고 집중하도록 망에 대한 인증과 권한을 허가합니다.

FreeRADIUS 는 모뎀을 리용한 인증쏘프트웨어를 개발하는 개발자들에게 도움을 줍니다.

특별한 자원요구는 제기되지 않으며 모뎀장치가 설치되여있어야 합니다.

– **용어 및 략어**

- 삽입인증모듈 (PAM: pluggable authentication module)
- 암호인증규약 (PAP:Password Authentication Protocol)
- 도전/맞잡이인증규약 (CHAP:Challenge/Handshake Authentication Protocol)

- 사용자등록부조직(UHO: User Home Organization)
- 동등형망(peer to peer)
- 대리순서(agent sequence)
- 견인순서(pull sequence)
- 천순서(push sequence)

– **기본필수패키지목록**

- 실행패키지목록

  Chkconfig
  net-snmp
  krb5-libs
  net-snmp-utils

- 원천패키지콤파일을 위한 패키지목록

  net-snmp-devel
  net-snmp-utils
  krb5-devel
  openldap-devel
  openssl-devel
  pam-devel
  libtool-ltdl-devel
  libtool
  gdbm-devel
  zlib-devel
  perl

– **mysql 련동패키지목록**

- 실행패키지목록

  Mysql

- 원천패키지콤파일을 위한 패키지목록

  mysql-devel

– **postgresql 련동패키지목록**

- 실행패키지목록

  Postgresql

- 원천패키지콤파일을 위한 패키지목록

  postgresql-devel

- **UnixODBC 련동패키지목록**

● 실행패키지목록
UnixODBC

● 원천패키지콤파일을 위한 패키지목록
UnixODBC-devel

2. 모뎀인증봉사기(Radius Server)의 설치

1) 설치

《붉은별》 봉사기용체계 3.0에는 기정으로 Radius 쏘프트웨어가 설치되여있습니다. 만일 새롭게 다시 설치하려면 다음과 같은 지령을 실행합니다.

rpm –ivh freeradius-2.1.9-3.rss3.rpm

2) . 쏘프트웨어의 구성관계

- **의뢰기화일(/etc/raddb/clients)**

이 화일은 의뢰기요청에 리용하는 주콤퓨터들의 비밀열쇠를 사용하여 FreeRADIUS 봉사기를 발견하기 위한 권한가진 주콤퓨터들을 렬거한 화일입니다. 의뢰기화일은 다음과 같이 볼수 있습니다.

실례:

```
# Client Name Key
#---------------- ----------
#portmaster1.isp.com testing123
#portmaster2.isp.com testing123
#proxyradius.isp2.com TheirKey
localhost testing123
192.168.1.100 testing123
 tc-clt.hasselltech.net oreilly
```

- **naslist 화일(/etc/raddb/naslist)**

이 화일에서는 nickname과 NAS 류형봉사기를 발견하기 위한 NAS 표준완전이름을 렬거합니다.

이 화일은 다음과 같습니다.

실례:

```
# NAS Name Short Name Type
#---------------- ---------- ----
#portmaster1.isp.com pm1.NY livingston
localhost local portslave
192.168.1.100 local portslave
```

tc-clt.hasselltech.net tc.char tc

- **naspasswd 화일(/etc/raddb/naspasswd)**

이 화일은 NAS 장치우의 checkrad 편의쏘프트웨어를 기동하여 누가 어느 포구에 기록하였는가를 알수 있도록 검사하는데 리용합니다. 일반적으로 SNMP 규약은 이렇게 할수 있지만 장치는 초기 checkrad 편의쏘프트웨어로부터 방조받으면서 렬거합니다. 이 화일은 다음과 같습니다.

실례:

206.229.254.15 !root JoNAThaNHasSELl
206.229.254.5 !root FoOBaR

- **hints 화일(/etc/raddb/hints)**

이 화일은 특정사용자를 위한 봉사를 준비하는 RADIUS 봉사기에 암시를 제공하는데 사용됩니다. 실례로 SLIP 접속을 위한 기정봉사를 구성할 때 SLIP 접속은 사용자가 그의 표준사용자이름으로 접속하면서 설치됩니다. 그러나 꼭같은 사용자가 ppp 접속을 바란다면 SLIP 사용자이름을 Prneis 로 고치고 RADIUS 봉사기(/etc/raddb/hints 화일로부터 변환)는 그를 위한 ppp 접속을 설치합니다.

이 화일은 다음과 같습니다.

실례:

```
DEFAULT Prefix = "P", Strip-User-Name = Yes
 Hint = "PPP",
 Service-Type = Framed-User,
 Framed-Protocol = PPP

DEFAULT Prefix = "S", Strip-User-Name = Yes
 Hint = "SLIP",
 Service-Type = Framed-User,
 Framed-Protocol = SLIP

DEFAULT Suffix = "P", Strip-User-Name = Yes
 Hint = "PPP",
 Service-Type = Framed-User,
 Framed-Protocol = PPP

DEFAULT Suffix = "S", Strip-User-Name = Yes
 Hint = "SLIP",
 Service-Type = Framed-User,
 Framed-Protocol = SLIP
```

- **huntgroup 화일(/etc/raddb/huntgroup)**

Huntgroup 는 RADIUS 의뢰기장치에 대한 포구 혹은 기타 통신출구모임입니다. FreeRADIUS 의 경우에 huntgroup 는 RADIUS 의뢰기장치의 특수한 일부를 포구모임으로 할수 있습니다. 또는 기타 포수로부터 분리하려는 담당 ID 호출모임으로 할수 있습니다. 이것은 정적 IP 주소할당을 가능하게 하고 특정의 huntgroup 에 사용자이름/암호를 정합하여 일정한 사용자와 집단에 접근을 제한하는 huntgroup 을 정의하여 이것들을 려파할수 있습니다.

Huntgroup 은 NAS 와 포구범위의 IP 주소에 기초하여 정의합니다. 이 화일을 구성하기 위하여 먼저 매 POP 에 말단봉사기를 지정할수 있습니다. 다음에 가능한 사용자가 제한을 안정하게 통과하게 하고 표준을 정의하는 구획으로 구성합니다.

실례:

```
raleigh NAS-IP-Address == 192.168.1.101
raleigh NAS-IP-Address == 192.168.1.102
raleigh NAS-IP-Address == 192.168.1.103
premium NAS-IP-Address == 192.168.1.101, NAS-Port-
 Id == 0-4
 Group = premium,
 Group = staff
```

- **users 화일 (/etc/raddb/users)**

FreeRADIUS 는 users 화일에서 알지 못하는 사용자서술의 초기 RADIUS 봉사기형태에 대한 몇개의 수정을 허가합니다.

항목들은 users 화일에서 나타나는 순서로 처리되며 일단 찾아 처리하면 RADIUS 처리를 중지합니다.

Fall-Through = yes 속성은 정합한 기초우에서 처리를 유지하도록 봉사기를 지시하는 설정입니다.

이 화일은 다음과 같습니다.

실례:

```
steve Auth-Type := Local, User-Password == "testing"
 Service-Type = Framed-User,
 Framed-Protocol = PPP,
 Framed-IP-Address = 172.16.3.33,
 Framed-IP-Netmask = 255.255.255.0,
 Framed-Routing = Broadcast-Listen,
 Framed-Filter-Id = "std.ppp",
 Framed-MTU = 1500,
 Framed-Compression = Van-Jacobsen-TCP-IP
DEFAULT Service-Type == Framed-User
```

Framed-IP-Address = 255.255.255.254,
Framed-MTU = 576,
Service-Type = Framed-User,
Fall-Through = Yes
DEFAULT Framed-Protocol == PPP
Framed-Protocol = PPP,
Framed-Compression = Van-Jacobson-TCP-IP

- **radiusd.conf 화일(/etc/raddb/radius.conf)**

이 화일은 FreeRADISU 제품의 기본동작을 위한 선택항목과 거의 모든 명령들을 렬거하는 Apache의 httpd.conf 화일과 같습니다.

Passwd, shadow, group 화일들의 위치를 서술하기 위하여 다음과 같이 서술합니다.

실례:

```
Unix {
 (some content removed)
 passwd = /etc/passwd
 shadow = /etc/shadow
 group = /etc/group
 (some content removed)
}
```

지령행으로부터 다음과 같이 raadiusd 대몬을 실행합니다.

실례:

```
#/etc/raddb/radius
Radius:Starting-rending configuration files…
```

3. 모뎀인증봉사기(Radius Server)의 작업절차

1) 봉사의 시작과 중지

- 봉사의 시작

작업을 시작하려면 다음의 지령을 입력합니다.

```
# service radiusd start
```

- 봉사의 중지

작업을 중지 및 중지하려면 다음의 지령을 실행합니다.

```
# service radiusd stop
```

2) 실행형식과 선택항목

– 실행형식

radiusd 대몬은 인증, 권한, 계산자리봉사기입니다. 실행형식은 다음과 갈습니다.

radiusd [-A] [-S] [-A accountingdirectory] [-b] [-c] [-d config directory] [-f] [-i ip-address] [-l logdirectory] [-g facility] [-p port] [-s] [-v] [-x] [-X] [-y] [-z]

FreeRADIUS 리행은 radius 봉사기쏘프트웨어입니다. 이 쏘프트웨어를 통하여 Livingston 의 radius 2.0 과 크게 량립할수 있으며 코드의 임의의 부분에 기초하지 않습니다.

FreeRADIUS 는 radius 봉사기의 성능과 구성을 제고할수 있습니다. 결과적으로는 복잡한 요청에 따라 체계구성이 어려울수 있습니다. 그러므로 다음의 단계에 따라 처리하여야 합니다.

- 항상 봉사기를 오유추적방식(radius –X)으로 실행시켜야 합니다. 만일 오유추적방식으로 실행하지 않는다면 동작상태를 볼수 없을 뿐만아니라 임의의 문제를 정확히 해결할수 없습니다.
- radius.conf 화일을 편집할 때 authorize{} 부분에서 가능한껏 변경을 적제하여야 합니다. 모듈들의 순서는 봉사기가 요청을 취급하는 방법을 자동적으로 처리할수 있는 림계상태이므로 모듈들의 순서변경은 봉사기가 동작할수 없게 할수 있습니다.
- 검사할 때 users 화일에서 사용자와 암호구성에 의한 기동을 시작하게 합니다. 봉사기가 그 사용자에 대하여 오래 등록하고있다면 그 사용자에 대한 암호를 지워야 합니다.
- 점차적으로 봉사기에 복잡한 구성을 추가합니다.

radius 는 봉사기접근사이의 규약을 말합니다. 보통 장치는 여러개의 모뎀 혹은 ISDN, 그리고 radius 봉사기와 련결됩니다. 사용자가 봉사기에 접근하려고 접속할 때 망가입이름과 암호를 요구합니다. 이 정보는 radius 봉사기에 전송됩니다. 봉사기는 접근거부 혹은 접근승인을 응답합니다. ppp 접속의 경우에 IP 주소와 같이 마지막에 망가입정보가 전송됩니다.

봉사기접근은 또한 radius 봉사기가 그러한 등록계산자리를 진행하도록 기록한 망가입과 망가입해제를 전송합니다. 이 기록은 개개의 말단봉사기를 분류하는 wtmp 화일에 유지되며 기록화일 /var/log/radwtmp 와 량립됩니다.

– 선택항목

-A: 같은 등록부에 있는 표준상세화일에 추가적으로 detail.auth 화일을 씁니다. 이 화일은 모든 인증요청기록을 포함합니다. Radius.conf 화일에서 detail 모듈에 대한 구성을 참고하십시오.

-S: 말단봉사기로부터 수신된 미가공기록대신에 상세화일에서 사용자이름(앞붙이와 뒤붙이 없이)을 붙여 씁니다. 이 지령선택항목은 radius.conf 화일에

서 log stripped names 구성항목을 보고 참고하십시오.

-a: accounting directory: 등록부는 기정적으로 /var/log/radacct 입니다. 만일 등록부가 존재하지 않으면 radius는 모든 login/logout 기록에 대한 상세화일안으로 계산자리기록을 씁니다. 상세화일의 위치는 acctdir/terminal_server/detail 입니다. 이 지령은 radius.conf 화일의 radacctdir 구성항목을 참고하십시오.

-l: logging directory: 등록부는 기정으로 /var/log 입니다. radius는 radius.log 라는 리력화일에 씁니다. 그것은 정보와 오유통보문, 그리고 임의의 모든 망가입시도기록을 포함합니다. 특수한 인수 stdout 와 stderr는 표준출력에 의하여 씌여진 정보 혹은 표준오유들입니다. 이 지령은 radius.conf 화일에서 log dir 구성항목을 참고하십시오.

-g: facility: -l syslog를 리용하는 syslog편의쏘프트웨어를 지정합니다. 기정으로 대몬이며 합리적인 authpriv를 선택합니다.

-d: config directory: 기정적으로 /etc/raddb 등록부입니다. radiusd는 dictionary 와 user 화일과 같은 구성화일을 찾습니다.

-i: ip-address: 다중가동환경을 가진 주콤퓨터에 대한 유용한 파케트송신과 수신을 위하여 결합하려는 IP 주소를 정의합니다. 이 지령은 radius.conf 화일에서 bind address 구성항목을 참고하십시오.

-b: 만일 radius 봉사기실행화일이 dbm을 지원하도록 콤파일되였다면 이 기발은 users 화일대신에 실지로 자료기지를 리용하도록 합니다.

-c: 기억기에 있는 해쉬표에서 password 와 group, shadow 화일을 캐시화합니다. radius는 기억기의 많은 비트를 리용하여 처리하지만 사용자이름은 암호화일에서 고속으로 탐색합니다. 실지 암호화일에서 모든 변경을 진행한 후에 그것들의 구성과 password/group/shadow 화일을 다시 읽어들이도록 radius 봉사기가 SIGHUP을 전송할 필요가 있습니다. 이 지령은 radiusd.conf 화일에서 Unix 모듈에 대한 cache 구성항목을 참고하십시오.

-f: 전처리를 진행하는 동안 가지치기를 하지 않습니다.

-p: port: 일반적으로 radiusd는 /etc/services(radius 와 radacct)에서 지정된 포구를 리용합니다. 이 선택항목을 리용하여 radiusd는 인증요청에 대한 지정된 포구와 등록계산자리요청에 대한 port+1 을 리용합니다. 이 지령은 radius.conf 화

일에서 port 구성항목을 참고하십시오.

-s: 하나의 봉사기방식으로 동작합니다. 봉사기는 일반적으로 요청에 대한 응답시간이 떨어지는 다중토막과제 and/or 처리로 동작합니다. 일부 체계들은 토막과제를 발생하고 하나의 봉사기방식에서 실행은 그 발행주소에 도움을 청합니다.

-v: 봉사기정보판본을 현시하고 탈퇴합니다.

-x: 오유추적방식입니다. 이 방식에서 봉사기는 stderr 출력에 대한 모든 요청의 상세한것을 현시합니다. –s 결합이 아주 유용합니다. 오유추적출력의 여러 비트를 얻기 위하여 이 선택항목을 두번 지정할수 있습니다.(-x -x 혹은 -xx)

-X: 확장오유추적방식입니다. –sfxx 와 동등합니다.

-y: radius.log 화일에 모든 인증요청에 대하여 상세한것을 기록합니다. 이 지령은 radius.conf 화일에 있는 logauth 구성항목을 참고하십시오.

-z: 망가입이 성공하면 radius.log 화일에 암호를 포함합니다. 이것은 매우 보안상 위험합니다. 이 지령은 radius.conf 화일에 있는 logauthbadpass 와 logauthgoodpass 구성항목을 참고하십시오.

3) 모뎀인증봉사기의 구성화일 설정

Radius 는 구성화일을 여러개 사용합니다. 매개 화일의 형식은 그 화일의 사용페지에 서술되여있습니다.

① radiusd.conf: 기본 구성화일로서 관리조종항목을 설정합니다.

② Dictionary: 이 화일은 보통 정적입니다. 기타 구성화일에서 리용하는 모두 가능한 RADIUS 속성을 정의합니다. 그것은 수정할수 없으며 같은 등록부에 있는 기타 dictionary 화일들을 포함합니다.

③ clients: 봉사기에 접속하려는 모든 의뢰기에 대한 IP 주소와 보안열쇠를 포함합니다.

④ naslist: 망에서 모든 NAS(Network Access Server)정보들을 포함합니다. 본질적으로 망에서 radius 대리봉사기를 가지는 경우 의뢰기와 같으면 안됩니다. 그 경우에 대리봉사기는 의뢰기이면서 다른 NAS에 대한 요청을 전송합니다.

또한 상세화일에 씌여진 사전이름을 작성하는데 리용하는 그리고 /var/log/radwtmp 화일에 리용하는 매 말단봉사기에 대한 생략이름을 포함합니다.

마지막으로 NAS 류형이 무엇인가를 정의합니다.(Cisco, Livingston, Portslave)

⑤ Hints: 봉사기를 거쳐서 전송되는 사용자의 망가입이름과 기타 속성에 기초하여 radius 봉사기에 정확한 암시를 정의합니다.
  또한 Livingston 2.0 봉사기가 users 화일에서 지원하는 prefix 와 suffix 의 기능을 제공합니다.

⑥ Huntgroups: 정확한 사용자(집단)를 위한 정확한 huntgroup 으로 접근을 제한하도록 가능하게 하는 huntgroup를 정의합니다.

⑦ Users: 여기에 사용자들이 정의됩니다. 표준설치에서 이 화일은 기본적으로 hints 화일로부터 암시에 기초한 여러개의 망가입류형을 처리하도록 DEFAULT 정보를 포함합니다. 인증은 UNIX /etc/passwd 화일내용에 기초합니다. 그러나 이 화일에 모든 사용자와 암호를 정의하는것으로써 가능합니다.

4) FreeRADIUS 고급설정

- PAM 리용

FreeRADIUS 는 삽입인증모듈인 PAM 을 제공하지만 그것은 번역시에 허가되여야 합니다. 그리고 현재 PAM 의 지원은 비표준입니다. 대부분의 RADIUS 배포판에서는 처리시 PAM 을 허가하기 위하여 users 화일에서 User-Password = PAM 으로 설정하지만 이것은 FreeRADIUS 에서는 지원되지 않습니다. 대신에 Auth-Type = Pam 으로 설정합니다. 다음의 실례는 사용자가 특정의 RADIUS 의뢰기로부터 망가입할 때 PAM 인증을 위하여 구성한 비특이성의 사용자를 위한 한부분입니다.

```
실례:DEFAULT Auth-Type := Pam, NAS-IP-Address ==
206.229.254.5
Service-Type = Framed-User,
Framed-Protocol = PPP,
Framed-IP-Address = 255.255.255.254,
Filter-Id = "20modun",
Framed-MTU = 1500,
Framed-Compression = Van-Jacobson-TCP-IP
```

일부 구성에서는 /etc/pam.d 화일에 특수한 정보마당들을 설정할수 있습니다. 다음의 users 화일구성은 특수 pam.d 마당을 위한 RADIUS 봉사기를 지적하는 유일한 “Pam-Auth=x”를 리용하는 부분입니다.

```
실례:DEFAULT Auth-Type := Pam,
Pam-Auth == "hasselltech-radius",
```

```
 NAS-IP-Address == 127.0.0.1
 Service-Type = Framed-User,
 Framed-Protocol = PPP,
 Framed-IP-Address = 255.255.255.254,
 Filter-Id = "15intonly",
 Framed-MTU = 1500,
Framed-Compression = Van-Jacobson-TCP-IP
```

이를 위해서 먼저 FreeRADIUS 설치를 시작할 때 PAM 지원을 허가하도록 번역프로그람의 설정을 구성하여야 합니다. Radiusssd.conf 화일을 열고 모듈부분으로 이행한 다음 모듈구동쏘프트웨어내부에서 pam 을 조사하여 PAM 동작을 허가합니다. Pam_auth 문자렬값은 /etc/pam.d 등록부에 있는 화일과 일치합니다.

```
pam {
       …
 pam_auth = radius
 …
}
```

같은 화일에서 인증부분으로 이행하여 pam 행을 능동으로 합니다.

```
authenticate {
 pam
 Unix
# ldap
# mschap
# eap
}
```

같은 화일에서 인증부분으로 이행하여 pam 행을 능동으로 합니다.

이제 /etc/pam.d 등록부로 가서 radius.conf 내부에 있는 pam 부분에 지정된 같은 이름을 리용하여 화일을 작성합니다. 이 새로운 화일에 다음의 행을 삽입합니다.

```
#%PAM-1.0
auth required /lib/security/pam_Unix_auth.so shadow md5 nullok
auth required /lib/security/pam_nologin.so
account required /lib/security/pam_Unix_acct.so
password required /lib/security/pam_cracklib.so
password required /lib/security/pam_Unix_passwd.so shadow md5 nullok use_authtok
session required /lib/security/pam_Unix_session.so
```

－ 대리봉사와 령역

FreeRADIUS는 대리봉사기로서 동작할수 있습니다. 적당한 구문을 구성하기 위하여 radius.conf 화일의 령역모듈부분을 참고하십시. 계속하여 령역구성은 /etc/raddb/proxy.conf 화일에서 진행합니다. 또한 /etc/raddb/realms 화일이 있지만 이것은 이러한 기능을 확장하는데 리용합니다. Proxy.conf 화일은 여러가지 설정과 인증주콤퓨터에 속하는 인증령역의 대리봉사기능을 위한 상세구성방향을 지적합니다. 령역 ralint를 위하여 proxy.conf 화일에 다음의 값들을 추가합니다.

```
realm ralint {
 type = radius
 authhost = radius.raleighinternet.com:1645
 accthost = radius.raleighinternet.com:1646
 secret = triangle
 nostrip
}
```

또한 대리봉사하지 않는 국부인증령역을 구성할수 있습니다.

```
realm durhamnet {
 type= radius
 authhost= LOCAL
 accthost= LOCAL
}
```

NULL 령역은 령역지정없이 인증요청을 사용할수 있습니다.

```
realm NULL {
 type= radius
 authhost= radius.raleighinternet.com:1645
 accthost= radius.raleighinternet.com:1646
 secret= triangle
}
```

마지막으로 DEFAULT 정보는 명백치 않은 콤퓨터에 대한 기타 령역에 적용합니다.

```
realm DEFAULT {
 type= radius
 authhost= radlocal.corp.raleighinternet.com:1645
 accthost= radlocal.corp.raleighinternet.com:1646
```

```
 secret= iamnotamicrosoftmachine
}
```

－ clients.conf 화일의 리용

FreeRADIUS 는 clients.conf 화일을 리용하여 대리봉사기로서 동작할수 있습니다. Clients.conf 화일에는 의뢰기와 NAS 류형에 대한 두개의 정보마당들이 있습니다. 의뢰기는 기본 인증스크립트에 사용되는 표준요청자입니다. 의뢰기정보마당의 경우에 정규적인 이름 혹은 초기원천 IP 주소를 clients.conf 에서 정보마당과 정합하고 비밀은 요청모임의 변화를 비교하는것입니다.

NAS 정보마당은 실지 NAS 나 기타 의뢰기류형들의 위치에 대하여 사용됩니다. NAS 는 어느 요청정보에 의하여 특징이 변화되였는가를 정보마당을 가지고 비교합니다. 즉 초기원천요청에 있는 NAS-IP-Address 속성을 리용하여 적당한 마당과 정합하고 NAS-Ident 속성을 변경시킵니다.

```
client 172.16.1.55 {
 secret = donttellanyone
 shortname = totalcontrol
 vendor = 3comusr
 type = tc
 login = !root
 password = changeme
nas 172.16.1.66 {
 secret = iamanas
 shortname = max6000
 vendor = lucent
 type = ascend
 login = !root
 password = changeme
```

－ MySQL 과의 련동

FreeRADIUS 는 MySQL 의 사용자자료기지에 대한 인증을 허가할수 있게 설치할수 있습니다. MySQL 을 리용하여 자료기지안에서 users 화일의 내용을 꺼내고 대신에 매 사용자마다 분리된 단락별로 사용자정보를 모두 보관합니다. 자료는 여러개의 개별적인 자료기지표로 존재하여야 합니다.

- 먼저 RADIUS 봉사를 위한 MySQL을 내리적재하고 콤파일 한 다음 설치합니다.
- 다음에 FreeRADIUS를 내리적재하고 콤파일하고 설치합니다.
- RADIUS 체계를 구성하기 위하여 쉘에서 인증목적을 위한 사용자를 추가합니다.(보통 사용자와 집단을 radius 로 합니다.)

일단 MySQL 을 설치한 다음 사용자자료기지를 위한 구조도식을 창조합니다. 필요한 마당을 가진 SQL 자료기지를 쉽게 만들어주는 지령스크립트화일이 표준 FreeRADIUS 배포판에 존재합니다.

{unpacked}/src/modules/rlm_sql/drivers/rlm_sql_mysql 등록부안에 이 스크립트화일인 db_mysql.sql 화일을 찾을수 있습니다.

다음의 쉘지령을 실행합니다.

```
# mysql -u{root} -p{rootpass} radius < db_mysql.sql
```

{root}는 RADIUS/MySQL 호상작용을 위하여 구성한 root 사용자 혹은 사용자이름이고 {rootpass}는 사용자암호입니다.

다음에 /etc/raddb/radius.conf 화일을 열고 모든 RADIUS 기능을 위한 SQL 을 사용하도록 FreeRADIUS 를 지시합니다.

- Suffix 와 files 마당사이에 있는 authorize 부분에 sql을 추가합니다.
- Unix 와 radutmp 사이에 있는 accounting 부분에 혼합하여 sql을 추가합니다.

실례:

```
authorize {
 preprocess
# counter
# attr_filter
# eap
 suffix
 sql
 files
# mschap
}

accounting {
# acct_unique
 detail
 # counter
 Unix
 sql
 radutmp
# sradutmp
}
```

- /etc/raddb/sql.conf 에 다음의 실례와 같이 MySQL사용자자료기지를 구성하는 사용자이름과 암호를 추가합니다.

```
sql {
# Database type
```

```
# Current supported are: rlm_sql_mysql, rlm_sql_postgresql,
# rlm_sql_iodbc, rlm_sql_oracle, rlm_sql_Unixodbc
driver = "rlm_sql_mysql"

# Connect info
server = "localhost"
login = "root"
password = "rootpass"

# Database table configuration
radius_db = "radius"

# If you want both stop and start records logged to the
# same SQL table, leave this as is. If you want them in
# different tables, put the start table in acct_table1
# and stop table in acct_table2
acct_table1 = "radacct"
acct_table2 = "radacct"

authcheck_table = "radcheck"
authreply_table = "radreply"

groupcheck_table = "radgroupcheck"
groupreply_table = "radgroupreply"

usergroup_table = "usergroup"

# Remove stale session if checkrad does not see a double login
deletestalesessions = yes

# Print all SQL statements when in debug mode (-x)
sqltrace = yes
sqltracefile = ${logdir}/sqltrace.sql
```

이제 자료기지를 가지고 작업하기 위하여 다음의 단계를 진행합니다.

usergroup 표에 사용자계산자리이름과 집단이름을 정합하는 정보마당을 작성합니다.

- radcheck표에 1 단계에서 작성한 사용자이름의 개별적인 정보마당을 작성하고 password 속성에 그것들의 암호를 지정합니다. Op 마당은 비여둡니다.
- radreply표에 FreeRADIUS가 인증요청에 응답할 때 돌려주는 특정속성에

사용자이름을 정합합니다.

- 마지막으로 radgroupreply 내부에 요청이 사용자로부터 일정한 집단을 만들 때 정합하는 응답을 작성합니다.

제14절. Java 웨브응용쏘프트웨어봉사기(Tomcat Server)

이 절에서는 Tomcat 사용자들에게 Tomcat 봉사기의 설치 및 시작방법과 관리도구사용방법에 대하여 설명합니다.

1. Java 응용쏘프트웨어봉사기의 개요

Tomcat 봉사기는 Java 웨브응용쏘프트웨어를 기동시키기 위한 Java 응용쏘프트웨어 봉사기입니다. 《붉은별》 봉사기용체계 3.0에 포함된 Tomcat 7.0.2는 Java Servlet와 JSP를 기동시키기 위한 Java 웨브응용쏘프트웨어봉사기입니다.

Tomcat 봉사기를 사용하면 Java 웨브응용쏘프트웨어들을 기동시킬수 있으며 Tomcat 관리도구를 리용하여 봉사기에 대한 관리를 진행할수 있습니다.

Tomcat 봉사기를 기동하려면 Java 가동환경이 설치되여있어야 합니다.

Tomcat는 Servlet와 JSP 개발자들이 시험봉사기로서 리용할수 있는 무료로 제공되는 Servlet 포함기이며 표준 Servlet와 JSP 응용쏘프트웨어대면부명세에 기초하고있기때문에 Java Servlet나 JSP를 리용한 동적인 웨브페지를 작성하는 경우 봉사기로서 리용할수 있습니다.

- 용어 및 략어

Java

Sun microsystem 회사가 개발한 쏘프트웨어작성언어입니다.

JRE**(Java Runtime Environment)**

Java 응용쏘프트웨어를 실행시키기 위한 가동환경입니다.

JSP

동적인 웨브페지를 만들수 있는 방법과 웨브응용쏘프트웨어를 간단히 작성, 처리할수 있게 해주는 Java 언어에 기초한 봉사기측 스크립트언어입니다.

Servlet

봉사기에서 쏘프트웨어를 처리하고 그 결과를 의뢰기에 전송하는 Java 언어에 기초한 쏘프트웨어입니다.

JVM (Java Virtual Machine) : Java 가상기계입니다.

2. 패키지 설치와 해제

1) 화일목록

Java 웨브응용쏘프트웨어를 기동시키기 위하여서는 다음의 화일이 설치되여 있어야 합니다.

- java-1.6.0-openjdk-1.6.0.0-1.21.b17.RSS3.i686.rpm

2) 쏘프트웨어 구성관계

-Tomcat 봉사기는 본체, 관리도구로 구성됩니다.

- Tomcat 본체: Tomcat 봉사와 관련한 기본기능들이 포함됩니다.
- Tomcat 관리도구: Tomcat 를 관리하는데 필요한 도구가 포함됩니다. 관리도구에는 Tomcat 관리자가 있습니다.

Tomcat 관리자: Tomcat 봉사기관리에 필요한 응용쏘프트웨어경로들과 전개기능 등을 제공합니다.

※ 관리도구를 리용하려면 해당한 CATALINA_HOME/conf/tomcat-users.xml 에서 사용자설정을 진행하여야 합니다.

3) 호출특성과 보안관련 특성

Tomcat 관리자사용을 위한 통과암호는 CATALINA_HOME/conf/tomcat-users.xml 에서 설정합니다.

Tomcat-users.xml 화일안에 다음의 역할을 추가하는것으로 Tomcat 봉사기관리를 진행할수 있습니다.

tomact 관리자에는 manager-gui 역할을 가진 사용자가 접근할수 있습니다.

아래에서는 tomcat-users.xml 구성화일안에서 manager-gui 역할을 가진 tomcat 사용자(암호:tomcat)를 설정한 실례를 보여줍니다.

```
<role rolename="tomcat"/>
<role rolename="role1"/>
<role rolename="manager-gui"/>
<role rolename="manager-script"/>
<user username="tomcat" password="tomcat" roles="tomcat, manager-gui "/>
<user username="both" password="tomcat" roles="tomcat,role1"/>
<user username="role1" password="tomcat" roles="role1"/>
```

4) 패키지 설치 및 해제

Tomcat 는《붉은별》 봉사기용체계 3.0 제품에 포함되여있습니다. 그러므로《붉은별》 봉사기용체계 3.0 을 설치하는 경우 표준으로 설치됩니다.

－ 수동으로 설치하는 경우 다음과 같은 순서로 설치를 진행합니다.

- Java의 설치

조작탁에서 다음의 지령을 실행하여 Java 가동환경을 설치합니다.

\# rpm ivh java-1.6.0-openjdk-1.6.0.0-1.21.b17.RSS3.i686.rpm

- Tomcat의 설치

조종탁에서 다음의 지령을 실행합니다.
32 비트판본: #rpm –ivh tomcat-7.0-kp.RSS3.i686.rpm
64 비트판본: #rpm –ivh tomcat-7.0-kp.RSS3.x86_64.rpm

Tomcat 가 정확히 설치되면 /usr/java/apache-tomcat 에 Tomcat 관련화일들 이 배치됩니다.

- 다음의 지령으로 설치된 Tomcat 를 해제합니다.
  #rpm –e tomcat-7.0-kp.RSS3.i686.rpm

3. Java 응용쏘프트웨어봉사기의 작업절차

1) 봉사의 시작과 중지

- 봉사의 시작
  - 조종탁에서 다음의 지령을 입력하여 Tomcat 를 시작합니다.
    #service tomcat7 start
  - 《빛발》3.0 에서 Tomcat 관리항목에서 《봉사기기동》단추를 누릅니다.

참고: Tomcat봉사기가 정확히 동작하면 *《http://Tomcat가 설치된 콤퓨터의 IP주소:8080》*을 호출하는 경우 Tomcat기동화면이 현시됩니다.

주의 : Tomcat봉사기가 기동하지 않는 경우 Tomcat 기동후 첫페지가 현시되지 않는 경우 다음의 지령으로 방화벽을 중지시켜주십시오. #service iptables stop

주의: **Tomcat 기록을 볼수 없는 경우** Tomcat 기록은 보안방책이 설정된 상태에서 볼수 없습니다. 기록을 보려면 보안방책을 해제하여야 합니다. 보안방책해제와 관련한 구체적인 지령은 보안방책지도서를 참고하십시오.

- 봉사의 중지
  - 조종탁에서 다음의 지령을 입력하여 Tomcat 를 중지합니다.
    #service tomcat7 stop

- 《빛발》3.0 에서 Tomcat 관리항목의 《봉사기중지》단추를 누릅니다.

2) 사용방법

Tomcat 에서 사용하는 웨브응용쏘프트웨어는 Servlet 와 JSP 명세에 따릅니다.
JavaServlet 명세는 WAR 화일형식과 여러가지 목적의 구조를 정의합니다. 웨브응용쏘프트웨어를 사용하려면 웨브페지와 구성화일 등을 저장하기 위한 등록부배치와 같은 일정한 관습에 따라야 합니다. 일반적인 배치는 다음과 같습니다.

```
/
/index.jsp
/products.jsp
/widgets/index.html
/widgets/pricing.jsp
/images/logo.png
/WEB-INF/web.xml
/WEB-INF/classes/com/acme/PriceServlet.class
/WEB-INF/classes/DataHelper.class
/WEB-INF/lib/acme-util.jar
```

우에서 보는바와 같이 웨브페지의 내용들은 웨브응용쏘프트웨어의 뿌리등록부와 해당한 보조등록부에 배치될수 있습니다. 화상화일들은 /images 보조등록부에 배치될수 있습니다.
WEB-INF 등록부는 몇가지 특정한 내용들을 포함합니다.
classes 등록부는 Servlet, JSP 나 기타 응용쏘프트웨어코드부분에서 사용하는 Servlet 나 기타 클라스들과 같은 Java 클라스화일들을 포함합니다.
lib 등록부는 클라스패키지들을 포함하는 Java 압축화일(JAR)를 배치하는곳입니다.
web.xml 화일에는 웨브응용쏘프트웨어에 대한 구성과 응용쏘프트웨어서술, 전용화에 필요한 추가적인 내용들을 포함합니다.

① 처리절차들

처리는 다음과 같이 진행됩니다.

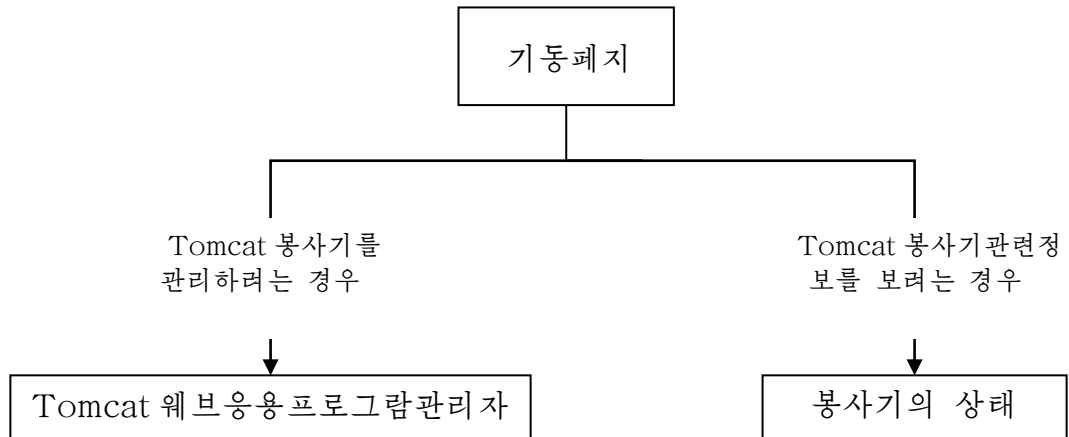



그림 28. 처리구성도

② 사용방법

－ 기동페지의 현시

봉사기가 기동된 상태에서 열람기의 주소칸에 http://Tomcat 가 설치된 콤퓨터 IP 주소:8080 을 호출하면 다음의 기동페지가 현시됩니다.

Apache Tomcat 7.0.2

이 홈페지가 열려진것은 Tomcat가 정확히 기동하였다는것을 의미합니다.

이것은 기정의 홈페지로서 다음의 경로에서 찾을수 있습니다:

$CATALINA_HOME/webapps/ROOT/index.html

여기서 "$CATALINA_HOME" 은 Tomcat가 설치된 뿌리등록부입니다.

문서

Tomcat 문서

주의: 보안상리유로 관리자웨브응용프로그람의 사용은 "manager-gui"의 역할을 가진 사용자만이 사용할수 있습니다.

다음의 화일을 참고하십시오:

$CATALINA_HOME/conf/tomcat-users.xml

기타

Servlet실례

JSP실례

이 배포물에는 Servlet와 JSP의 실례(원천코드포함)들과 웨브응용프로그람을 개발하는데 필요한 기타 안내문서들이 있습니다.

그림 29. Tomcat 기동페지

《기동페지》를 통하여 Tomcat 웨브응용프로그람관리페지, 봉사기상태보기페지와 같은 관리페지와 Tomcat 사용지도서, Java 웨브응용쏘프트웨어실례에로 갈수 있습니다.

참고1 : 기동페지가 정확히 현시되는가를 통하여 Tomcat봉사기기동을 확인할 수 있습니다.

– 웨브응용쏘프트웨어관리

Tomcat 에 설치된 웨브응용쏘프트웨어는 《Tomcat 웨브응용프로그람관리자》 페지에서 관리할수 있습니다.

– 《Tomcat 웨브응용프로그람관리자》페지의 호출

- 《기동페지》의 《관리》항목에서 《Tomcat 웨브응용프로그람관리자》를 선택합니다.
- 사용자이름과 통과암호를 물어보는 창이 현시되면 Tomcat 웨브응용프로그람관리권한을 가진 사용자이름과 통과암호를 입력하고 《확인》단추를 누릅니다.
- 사용자이름과 통과암호가 정확하면 아래의 그림과 같은 《Tomcat 웨브응용프로그람관리자》페지가 현시됩니다.

Tomcat 웨브응용프로그람관리자

통보	확인

관리자			
응용프로그람일람	HTML관리자도움말	관리자도움말	봉사기의 상태

경로	이름	실행중	세션	지령
/	Tomcat기동페지	true	0	기동 정지 다시적재 전개해제 세션 기한초과 초과시간: 30 분이상
/docs	Tomcat 문서	true	0	기동 정지 다시적재 전개해제 세션 기한초과 초과시간: 30 분이상
/examples	써블레트와 JSP 실례들	true	0	기동 정지 다시적재 전개해제 세션 기한초과 초과시간: 30 분이상
/manager	Tomcat 관리자응용프로그람	true	3	기동 정지 다시적재 전개해제 세션 기한초과 초과시간: 30 분이상

전개

봉사기우의 WAR화일 또는 등록부의 전개

상황경로(생략가능):

XML 설정화일의 URL:

WAR화일 또는 등록부의 URL:

전개

WAR화일의 전개

올리적재하는 WAR화일선택 Browse...

전개

그림 30. Tomcat 웨브응용쏘프트웨어관리자페지

참고 2: 관리자권한의 설정방법

Tomcat 봉사기를 관리할수 있는 관리자들에 대한 권한은 CATALINA_HOME/conf/tomcat-users.xml 에서 설정할수 있습

니다. 구체적인것은 **2. 3)**의 **호출특성과 보안관련특성**을 참고하십시오.

《Tomcat 웨브응용프로그람관리자》 페지를 리용하여 사용자는 봉사기에 설치된 웨브응용쏘프트웨어에 대하여 다음과 같은 관리를 진행할수 있습니다.

- 웨브응용쏘프트웨어 시작
- 웨브응용쏘프트웨어 중지
- 웨브응용쏘프트웨어 다시적재
- 웨브응용쏘프트웨어 전개해제
- 웨브응용쏘프트웨어 전개
- 기억기루실검사

구체적인 사용방법은 다음과 같습니다.

- 웨브응용쏘프트웨어 시작

  중지된 웨브응용쏘프트웨어를 선택하고 《기동》단추를 누릅니다.
- 웨브응용쏘프트웨어 중지

  기동중의 웨브응용쏘프트웨어를 선택하고 《중지》단추를 누릅니다.
- 웨브응용쏘프트웨어 다시적재

  다시적재하려는 웨브응용쏘프트웨어를 선택하고 《다시적재》단추를 누릅니다.
- 웨브응용쏘프트웨어 전개해제

  전개해제하려는 웨브응용쏘프트웨어를 선택하고 《전개해제》단추를 누릅니다.
- 웨브응용쏘프트웨어 전개

  웨브응용쏘프트웨어의 전개는 다음의 두가지 방식이 있습니다.

- 봉사기에 존재하는 WAR 화일이나 등록부의 전개

《전개》항목의 《봉사기우의 WAR 화일 또는 등록부의 전개》에서 상황경로와 XML 설정화일경로, WAR 화일이나 등록부의 URL 을 입력하고 《전개》단추를 누릅니다.

- 의뢰기에 존재하는 WAR 화일의 전개

《전개》항목의 《WAR 화일의 전개》에서 《올리적재하려는 WAR 화일 선택》에 전개하려는 WAR 경로를 입력하고 《전개》단추를 누릅니다.

주의: 전개하는 WAR화일의 형식

전개하는 WAR화일의 형식은 확장자가 .war로 되여 있어야 합니다.

- 기억기루실검사

《진단》항목의 《루실찾기》단추를 누릅니다.

－ 봉사기상태 보기
봉사기관련정보들은 《봉사기의 상태》페지에서 찾을수 있습니다.

－ 《봉사기의 상태》페지호출

① 《기동페지》의 《관리》항목에서 《상태》를 선택합니다.

② 사용자이름과 통과암호를 물어보는 창이 현시되면 상태보기권한을 가진 사용자이름과 통과암호를 입력하고 《확인》단추를 누릅니다.

※ 봉사기관리권한설정은 《참고 2: **관리자권한의 설정방법**》을 참고하십시오.

③ 사용자이름과 통과암호가 정확하면 아래의 그림과 같은 《봉사기의 상태》페지가 현시됩니다.

봉사기의 상태

관리자			
응용프로그람일람	HTML관리자도움말	관리자도움말	봉사기의 모든 상태

봉사기정보

Tomcat판번호	JVM판번호	JVM제작자	조작체계이름	핵심부판번호	조작체계구성방식
Apache Tomcat/7.0.2	1.6.0_17-b17	Sun Microsystems Inc.	붉은별(봉사기용)	2.6.32-120727.RSS3.i686	i386

Java가상기계

여유기억기: 31.45 MB 전체기억기: 39.31 MB 최대기억기: 464.18 MB

http-8080

최대쓰레드수: 200 현재 쓰레드수: 10 현재 가동중인 쓰레드수: 1
최대처리시간: 113 ms 처리시간: 0.314 s 요청개수: 11 오유개수: 1 수신된 바이트수: 0.00 MB 전송된 바이트수: 0.05 MB

단계	시간	전송된 바이트수	수신된 바이트수	의뢰기	가상주콤퓨터	요청
S	1 ms	0 KB	0 KB	192.168.1.132	192.168.1.116	GET /manager/status HTTP/1.1

P: 요청해석 및 준비 S: 봉사 F: 완료 R: 준비 K: 활성

ajp-8009

최대쓰레드수: 200 현재 쓰레드수: 0 현재 가동중인 쓰레드수: 0
최대처리시간: 0 ms 처리시간: 0.0 s 요청개수: 0 오유개수: 0 수신된 바이트수: 0.00 MB 전송된 바이트수: 0.00 MB

단계	시간	전송된 바이트수	수신된 바이트수	의뢰기	가상주콤퓨터	요청

P: 요청해석 및 준비 S: 봉사 F: 완료 R: 준비 K: 활성

그림 31. 봉사기의 상태페지

봉사기의 상태페지에서는 다음과 같은 봉사기정보들을 열람할수 있습니다.

- 조작체계정보

조작체계의 물리기억기크기, 사용가능한 기억기크기, 전체 페지화일 크기, 여유페지화일크기, 기억기적재, 처리핵심부시간, 처리사용자시간을 열람할수 있습니다.

- Java 가상기계정보

여유기억기크기와 전체기억기크기, 최대기억기크기를 열람할수 있습니다.

- http-8080 정보

최대쓰레드수, 현재 쓰레드개수, 가동중의 쓰레드수, 가동중의 소케트수, 최대처리시간, 처리시간, 요청개수, 접수된 바이트수, 보낸 바이트수에 대한 정보를 열람할수 있습니다.

- Ajp-8009 정보

최대쓰레드수, 현재 쓰레드개수, 가동중의 쓰레드개수, 가동중의 소케트개수, 최대처리시간, 처리시간, 요청개수, 오유개수, 접수된 바이트수, 보낸 바이트수에 대한 정보를 볼수 있습니다.

4. 낮은 판본의 Java 응용쏘프트웨어봉사기와의 호환

기존웨브응용프로그람을 새 판본의 Tomcat 에로 이행하는 경우 기동이 잘 안되는 대부분의 원인은 Tomcat 에서 가동하는 웨브응용프로그람들이 여러가지 Java 서고들을 리용하기때문입니다. 그러므로 서고파일들을 적절히 선택하여 사용한다면 기동에서 제기되는 문제를 해결할수 있습니다.

여기서는 새판본으로 이행하는 과정에 자주 제기되는 문제들을 실례로 들고 기존웨브응용프로그람을 새 판본에로 이행하는 과정에 진행하여야 할 작업내용들을 종합하여 설명합니다.

1) 웨브응용프로그람내부문제

실례에 들어가기 앞서 Tomcat 관련 모든 오유들은 /usr/java/apache-tomcat/logs 에 기록된다는것을 명심해주십시오. 그러므로 홈페지가 정확히 기동하지 않는 경우 기록을 보면서 오유를 추적해나갈수 있습니다. 기록을 볼수 없는 경우에는 《주의: Tomcat 기록을 볼수 없는 경우》를 참고해주십시오.

실례 1 :홈페지(홈페지원천위치 /ROOT 라고 가정)가 기동하지 않으며 war 파일이 전개되지 않습니다./usr/java/apache-tomcat/logs/catalina.out 에는 다음과 같은 오유가 출력되였습니다.

```
2013. 6. 29 오후 4:37:07 org.apache.catalina.loader.WebappClassLoader val
idateJarFile
정보: validateJarFile(/usr/java/apache-tomcat/webapps/ams/WEB-INF/lib/s
```

```
ervlet-api.jar) - jar not loaded. See Servlet Spec 2.3, section 9.7.2. Offending cl
ass: javax/servlet/Servlet.class
   2013. 6. 29 오후 4:37:07 org.apache.tomcat.util.digester.Digester endEleme
nt
   심각: End event threw exception
   java.lang.NoSuchMethodException: org.apache.catalina.deploy.WebXml ad
dFilter
   at org.apache.tomcat.util.IntrospectionUtils.callMethod1(IntrospectionUtils.
java:802)
   at org.apache.tomcat.util.digester.SetNextRule.end(SetNextRule.java:202)
   at org.apache.tomcat.util.digester.Digester.endElement(Digester.java:1058)
   at com.sun.org.apache.xerces.internal.parsers.AbstractSAXParser.endEleme
nt(AbstractSAXParser.java:604)
   at com.sun.org.apache.xerces.internal.impl.XMLDocumentFragmentScanne
rImpl.scanEndElement(XMLDocumentFragmentScannerImpl.java:1750)
   at com.sun.org.apache.xerces.internal.impl.XMLDocumentFragmentScanne
rImpl$FragmentContentDriver.next(XMLDocumentFragmentScannerImpl.jav
a:2906)
   at com.sun.org.apache.xerces.internal.impl.XMLDocumentScannerImpl.nex
t(XMLDocumentScannerImpl.java:624)
   at com.sun.org.apache.xerces.internal.impl.XMLDocumentFragmentScanne
rImpl.scanDocument(XMLDocumentFragmentScannerImpl.java:486)
   at com.sun.org.apache.xerces.internal.parsers.XML11Configuration.parse(X
ML11Configuration.java:810)
   at com.sun.org.apache.xerces.internal.parsers.XML11Configuration.parse(X
ML11Configuration.java:740)
   at com.sun.org.apache.xerces.internal.parsers.XMLParser.parse(XMLParser.
java:110)
   at com.sun.org.apache.xerces.internal.parsers.AbstractSAXParser.parse(Abs
tractSAXParser.java:1208)
   at com.sun.org.apache.xerces.internal.jaxp.SAXParserImpl$JAXPSAXPars
er.parse(SAXParserImpl.java:525)
   at org.apache.tomcat.util.digester.Digester.parse(Digester.java:1544)
```

출력결과에서 보다싶이 servlet-api.jar 를 적재하지 못하고 web.xml 에서 addFilter 라는 메쏘드를 찾지 못하였습니다.

해결방도

/usr/java/apache-tomcat/lib 등록부와 /usr/java/apache-tomcat/webapps/ROOT/WEB-INF/lib 등록부에 다같이 catalina.jar 와 servlet-api.jar 가 존재하는것을 알수 있습니다. 결국 판본이 낮은 catalina.jar 와 servlet-api.jar 가/usr/java/apache-tomcat/webapps/ROOT/WEB-INF/lib 에 존재함으로써 생긴 오유입니다.

따라서 /usr/java/apache-tomcat/webapps/ROOT/WEB-INF/lib 등록부에서 catalina.jar 와 servlet-api.jar 를 삭제합니다.

실례 2: 홈페지(홈페지원천위치 /ROOT 라고 가정)가 기동하지 않으며 catalina.out 의 출력내용은 다음과 같습니다.

```
    2013. 6. 29 오후 5:28:42 org.apache.catalina.core.AprLifecycleListener init
    정보: The APR based Apache Tomcat Native library which allows optimal pe
rformance in production environments was not found on the java.library.path: /u
sr/lib/jvm/java-1.6.0-openjdk-1.6.0.0/jre/lib/i386/client:/usr/lib/jvm/java-1.6.0-o
penjdk-1.6.0.0/jre/lib/i386:/usr/lib/jvm/java-1.6.0-openjdk-1.6.0.0/jre/../lib/i38
6::/usr/java/apache-tomcat/lib:/usr/java/packages/lib/i386:/lib:/usr/lib
    2013. 6. 29 오후 5:28:42 org.apache.coyote.http11.Http11Protocol init
    정보: Coyote HTTP/1.1 을 http-8080 으로 초기화합니다
    2013. 6. 29 오후 5:28:42 org.apache.coyote.ajp.AjpProtocol init
    정보: Initializing Coyote AJP/1.3 on ajp-8009
    2013. 6. 29 오후 5:28:42 org.apache.catalina.startup.Catalina load
    정보: Initialization processed in 496 ms
    2013. 6. 29 오후 5:28:42 org.apache.catalina.core.StandardService startIntern
al
    정보: 봉사 Catalina 을(를) 기동합니다
    2013. 6. 29 오후 5:28:42 org.apache.catalina.core.StandardEngine startIntern
al
    정보: Starting Servlet Engine: Apache Tomcat/7.0.2
    2013. 6. 29 오후 5:28:42 org.apache.catalina.startup.HostConfig deployWAR
    정보: Web 응용프로그람등록부 trade.war 을(를) 배치합니다
    2013. 6. 29 오후 5:28:44 org.apache.catalina.core.StandardContext startIntern
al
심각: Error listenerStart
…
```

마지막행에 Error listenerStart 라는 통보문이 현시되였습니다. 이 상태에서 /log 등록부에 있는 localhost.2013-06-29.log 내용은 다음과 같습니다.

```
    2013. 6. 29 오후 5:28:44 org.apache.catalina.core.StandardContext listenerSt
art
    심각: 클라스 org.apache.myfaces.webapp.StartupServletContextListener 의
감시기실체에 상황초기화사건을 송신하는 과정에 오유가 발생하였습니다
    java.lang.NoClassDefFoundError: org/apache/commons/el/Logger
    at org.apache.myfaces.shared_impl.util.ClassUtils.<clinit>(ClassUtils.java:4
1)
    at org.apache.myfaces.config.FacesConfigurator.feedStandardConfig(FacesC
onfigurator.java:138)
    at org.apache.myfaces.config.FacesConfigurator.configure(FacesConfigurato
r.java:115)
    at org.apache.myfaces.webapp.StartupServletContextListener.initFaces(Startu
```

```
pServletContextListener.java:64)
    at org.apache.myfaces.webapp.StartupServletContextListener.contextInitializ
ed(StartupServletContextListener.java:47)
    at org.apache.catalina.core.StandardContext.listenerStart(StandardContext.jav
a:4323)
    at org.apache.catalina.core.StandardContext.startInternal(StandardContext.jav
a:4780)
    at org.apache.catalina.util.LifecycleBase.start(LifecycleBase.java:139)
    at org.apache.catalina.core.ContainerBase.addChildInternal(ContainerBase.ja
va:785)
```

출력결과에서 알수 있는것처럼 org/apache/commons/el/Logger 라는 메쏘트를 찾지 못하였습니다.

해결방도

이전판본의 Tomcat 의 lib 등록부(Tomcat 가 설치된 등록부안의 common/lib)에서 common-el.jar 를 복사하여 /usr/java/apache-tomcat/lib 에 복사하고 재기동합니다.

앞의 실례에서 본바와 같이 새판본의 Tomcat 리용시 제기되는 문제점은 홈페지리용에 필요한 서고들이 충돌하거나 정확히 추가하지 못했기때문에 생긴것들입니다.

이밖에도 도입시에는 대소문자구분문제, 홈페지경로문제 등이 제기될수 있습니다.

Tomcat7.0.2 에로 판본갱신할때 우에서 설명한 내용들을 주의해주십시오.

주의: **기존홈페지를 Tomcat7.0.2 에로 이행하는 방법**

① 운영중에 있는 기존 Tomcat 봉사기의 webapps 등록부안에서 해당한 웨브응용프로그람등록부(실례로 ROOT)를 Tomcat7.0.2 의 webapps 등록부(/usr/java/apache-tomcat/webapps)에 그대로 복사합니다.

② Tomcat7.0.2 에 복사한 웨브응용프로그람등록부안에 있는 lib 파일(실례에서 /usr/java/apache-tomcat/webapps/ROOT/WEB-INF/lib/)들중에서 Tomcat7.0.2 서고파일(/usr/java/apache-tomcat/lib)과 중복되는 파일들을 삭제합니다.

③ 운영중에 있던 기존 Tomcat 봉사기의 서고파일중에서 Tomcat7.0.2 와 중복되지 않는 파일들을 찾아 Tomcat7.0.2 서고등록부에 복사합니다.

2) 자료기지련동문제

홈페지기동시에 자주 제기되는 문제의 하나가 자료기지련동문제입니다.

《붉은별》(봉사기용)2.0 에서 정확히 동작하던 Java 웨브응용프로그람인 경우 자료기지와의 련동문제에서 자료기지봉사기문제와 JDBC 구동프로그람판본문제가 제기될수 있습니다.
자료기지와의 련동문제에서는 다음의 문제들을 확인해주십시오.
해당 자료기지가 정확히 동작하는가 확인하여야 합니다.
MySQL 자료기지인경우 MySQL 봉사기가 정확히 동작하고 있는가를 확인한 다음 필요한 자료기지에 정확히 접근가능한가를 확인하여야 합니다.
자료기지관리와 관련하여서는 봉사기사용지도서를 참고하여주십시오.
정확한 JDBC 구동프로그람을 사용하고 있는지 확인하여야 합니다.
《붉은별》(봉사기용)2.0 에서 가동하던 MySQL 은 판본이 5.0 계렬인 반면에 《붉은별》(봉사기용)3.0 에서 가동하는 MySQL 은 판본이 5.5 계렬입니다.
따라서 MySQL5.5 에 접속할수 있는 JDBC 구동프로그람을 사용하고 있는지 확인하여야 합니다.
JDBC 구동프로그람으로서는 mysql-connector-java-3.1.12-bin.jar 이상을 사용해주십시오.

자료기지와 관련하여 제기되는 오유역시 catalina.out 파일에 기록됩니다.
파일내용을 보면서 구동프로그람문제인지, 자료기지접근문제인지, 표접근문제인지 알수 있으므로 출력결과를 분석하면 오유를 퇴치할수 있습니다

제15절. 인쇄봉사기(CUPS)

이 사용지도서는 인쇄봉사기를 설치하고 리용하는데 필요한 사용방법들을 개괄하여 줍니다.

1. 인쇄봉사기의 개요

CUPS(Common Unix Printing System)는 본문편집기와 같은 여러가지 응용쏘프트웨어들에서의 인쇄작업을 관리하기 위하여 리용하는 인쇄봉사기 쏘프트웨어입니다. 응용쏘프트웨어들에서 인쇄하려는 페지내용을 인쇄기가 리해할수 있는 형식으로 변환하여 인쇄기에로 전송하면 인쇄기들은 들어온 요청순서로 대기렬에 들어있는 인쇄일감들을 인쇄합니다.
현재 인쇄기들의 종류가 다양하고 그 인쇄기들이 서로 다르게 동작하므로 인쇄작업은 매우 복잡합니다. CUPS 는 인쇄봉사의 복잡성을 숨기고 이 문제를 훌륭히 해결하여 간편한 인쇄기능을 쉽게 실현할수 있게 합니다.

1) 목적

인쇄봉사기란 말단사용자들에게 여러가지 형식으로 련결되여있는 다양한 형태의 인쇄기들을 편리하게 리용할수 있는 대면부를 제공하는 인쇄기관리봉사

기를 의미합니다. 인쇄기들은 USB 포구나 병렬포구를 통하여 직접 콤퓨터에 련결될수도 있으며 망을 통하여 련결될수도 있습니다. 또한 이와 같이 련결될수 있는 인쇄기들의 계렬과 자호 역시 여러가지 종류가 있습니다.

이 쏘프트웨어를 리용하면 말단사용자들에게는 인쇄기의 종류나 련결형식이 무엇인가에 상관없이 자체의 어느한 인쇄기로 보이게 하고 인쇄자료를 쉽게 인쇄할수 있습니다.

인쇄봉사기에서는 또는 어느 한 인쇄기에로 들어온 인쇄일감요청들을 감시하다가 지정한 일감을 잠간 중지시키거나 완전히 취소시키는것과 같은 여러가지 일감관리기능을 가지고있으며 일감이 끝났을 때 인쇄결과에 대하여 여러가지 방법으로 통지할수 있습니다.

이 쏘프트웨어는 이와 같은 기능들을 봉사기와 떨어진 말단에서 원격으로 접속하여 웨브페지형식으로 관리할수 있도록 편리한 관리대면부를 제공합니다.

이 사용지도서에서는 인쇄봉사기의 기본 구성화일에서 리용할수 있는 몇가지 구성항목들의 의미에 대해서 설명하고 원격으로 접속할수 있는 관리대면부를 리용하여 인쇄봉사기를 관리하고 리용하는 방법에 대하여 설명합니다.

2) 화일목록

cups-1.4.2-51.RSS3.i686.rpm
cups-devle-1.4.2-51.RSS3.i686.rpm
cups-libs-1.4.2-51.RSS3.i686.rpm
cups-lpd-1.4.2-51.RSS3.i686.rpm
enscript-1.6.4-15.RSS3.i686.rpm
foomatic-4.0.4-1.RSS3.i686.rpm
foomatic-db-4.0-7.20091126.RSS3.noarch.rpm
foomatic-db-filesystem-4.0-7.20091126.RSS3.noarch.rpm
foomatic-db-ppds-4.0-7.20091126.RSS3.noarch.rpm
ghostscript-8.70-6.RSS3.i686.rpm
ghostscript-fonts-5.50-23.1.RSS3.noarch.rpm
hpijs-3.9.8-33.RSS3.i686.rpm
hplip-3.9.8-33.RSS3.i686.rpm
hplip-common-3.9.8-33.RSS3.i686.rpm
hplip-libs-3.9.8-33.RSS3.i686.rpm
psutils-1.17-36.RSS3.i686.rpm

2. 인쇄봉사기의 설치

1) 설치

인쇄봉사기를 실현하는 기본적인 설치패키지들은 다음과 같습니다.

- cups-1.4.2-51.RSS3.i686.rpm

- cups-devel-1.4.2-51.RSS3.i686.rpm
- cups-libs-1.4.2-51.RSS3.i686.rpm
- cups-lpd-1.4.2-51.RSS3.i686.rpm
- hpijs-3.9.8-33.RSS3.i686.rpm
- hplip-3.9.8-33.RSS3.i686.rpm
- foomatic-4.0.4-1.RSS3.i686.rpm
- foomatic-db-4.0-7.20091126.RSS3.noarch.rpm
- ghostscript-8.70-6.RSS3.i686.rpm

여기에서 cups 패키지들은 기본적인 인쇄지령들과 함께 인쇄기를 관리하기 위한 대면부를 제공하는 쏘프트웨어입니다.

hpijs 와 hplip 패키지는 추가적인 인쇄기구동쏘프트웨어와 인쇄기구동쏘프트웨어서고들을 갖추고있는 쏘프트웨어입니다.

foomatic 및 foomatic-db 패키지는 각종 인쇄기들마다 특수하게 갖추고있는 자체의 인쇄양식, 인쇄서체 및 인쇄관련자료들을 자료기지화한 쏘프트웨어들로서 말단사용자들과 인쇄기사이의 호환성을 보장해주는 쏘프트웨어입니다.

ghostscript 는 인쇄자료를 인쇄기가 리용할수 있는 Postscript 형식의 사용지도서로 변환하는 변환쏘프트웨어들과 서고들을 갖추고있는 쏘프트웨어입니다.

우에서와 같은 인쇄봉사기쏘프트웨어들은 《붉은별》3.0 (봉사기용체계)를 완전설치할 때 체계에 자동적으로 설치됩니다.

인쇄봉사기쏘프트웨어를 설치하면 다음과 같은 등록부들이 체계에 설치됩니다.

- /etc/cups : cupsd.conf, printers.conf 와 같은 구성화일들이 있습니다.
- /usr/bin : 사용자쏘프트웨어들이 있습니다.
- /usr/include : CUPS 의 머리부화일들이 있습니다.
- /usr/lib : CUPS 의 서고화일들이 있습니다.
- /usr/lib/cups : 사용자 및 편의프로그람들과 같은 봉사기쏘프트웨어들이 있습니다.
- /usr/sbin : 관리쏘프트웨어들이 있습니다.
- /usr/share/cups : 서체와 같은 자료화일들이 있습니다.
- /usr/share/cups/www : 관리화일들이 있습니다.
- /usr/share/locale : 지역화화일들이 있습니다.
- /var/cache/cups : ppds.dat 와 remote.cache 와 같은 고속완충화일들이 있습니다.
- /var/log/cups : access_log, error_log 와 page_log 화일과 같은 기록화일들이 있습니다.
- /var/run/cups : 인증증명서화일과 령역소케트화일 및 상태자료들이 있습니다.

/var/spool/cups : 대기된 일감들이 있습니다.

2) 인쇄봉사기의 구성화일 설정

인쇄봉사기의 기본구성설정화일은 /etc/cups/cups.conf 화일입니다.
이 화일은 인쇄봉사기의 기능을 조종하는 구성항목들을 포함하고있습니다.
이 화일에서 리용할수 있는 구성항목들을 아래에서 간단히 설명합니다.

- **AccessLog**
  - 실례

AccessLog /var/log/cups/access_log
AccessLog /var/log/cups/access_log-%s
AccessLog syslog

  - 설명

AccessLog 는 접근기록화일이름을 설정합니다. 화일이름이 절대경로가 아니면 ServerRoot 등록부에서부터 상대경로로 간주합니다. 접근기록화일은 일반기록화일형식으로 저장되며 CUPS 봉사기의 동작정형을 알아볼수 있습니다.
%s 위치에 봉사기이름을 넣을수 있습니다.
평문화일대신 접근정보를 체계기록에 전송하기 위해 syslog 를 리용할수 있습니다.
기정접근화일은 /var/log/cups/access_log 입니다.

- **AccessLogLevel**
  - 실례

AccessLogLevel config
AccessLogLevel actions
AccessLogLevel all

  - 설명

AccessLogLevel 은 어떤 요청들을 접근기록화일에 기록하겠는가를 결정합니다. config 준위에서는 인쇄기들이나 클라스가 추가, 삭제, 변경되고 구성화일이 호출되거나 갱신되는 과정을 기록합니다.
actions 준위는 인쇄일감의 전송, 유지, 해방, 변경, 취소 및 임의의 구성조건에 대해서 기록합니다
all 준위는 모든 요청들을 기록합니다.
여기서 기정접근기록준위는 actions 입니다.

- **Allow**
  - 실례

```
<Location /path>
...
Allow from All
Allow from None
Allow from *.domain.com
Allow from .domain.com
Allow from host.domain.com
```

```
Allow from nnn.*
Allow from nnn.nnn.*
Allow from nnn.nnn.nnn.*
Allow from nnn.nnn.nnn.nnn
Allow from nnn.nnn.nnn.nnn/mm
Allow from nnn.nnn.nnn.nnn/mmm.mmm.mmm.mmm
Allow from xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx
Allow from @LOCAL
Allow from @IF(name)
</Location>
```

- 설명

Allow 는 봉사기에 접근이 허가된 주콤퓨터이름, IP 주소와 망을 지정합니다. Allow 는 여러개 리용할수 있으며 여러개의 망과 콤퓨터들의 접근을 허가하는데 리용할수 있습니다.

@LOCAL 은 모든 국부대면부들의 접근을 허용합니다. @IF(name)은 이름을 지적한 대면부들의 접근을 허용합니다. 두 경우에 CUPS 는 구성된 대면부들에 대해서만 접근을 허용하며 외부로부터 들어오는 요청들은 접수되지 않을것입니다. Allow 는 Location 나 Limit 절내에 있어야 합니다.

- **AuthType**
  - 실례

```
<Location /path>
...
AuthType None
AuthType Basic
AuthType Digest
AuthType BasicDigest
AuthType Negotiate
</Location>
```

- 설명

AuthType 는 다음과 같은 인증형태를 정의합니다:

- **None** - 인증하지 않습니다(기정값)
- **Basic** - Basic 인증은 Unix 체계암호화 집단화일을 통하여 진행됩니다.
- **Digest** - Digest 인증은 /etc/cups/passwd.md5 화일을 통하여 진행됩니다.
- **BasicDigest** - Basic 인증은 /etc/cups/passwd.md5 화일을 통하여 진행됩니다.
- **Negotiate** – Kerberos 인증으로 인증됩니다.

Basic, Digest, BasicDigest 나 Negotiate 인증을 리용할 때 localhost 대면부에 련결된 의뢰기들도 증명서를 통하여 인증할수 있습니다.

AuthType 은 Location 나 Limit 내에 있어야 합니다.

- **BrowseAllow**

- 실례

  BrowseAllow from all
  BrowseAllow from none
  BrowseAllow from 192.0.2
  BrowseAllow from 192.0.2.0/24
  BrowseAllow from 192.0.2.0/255.255.255.0
  BrowseAllow from *.domain.com
  BrowseAllow from @LOCAL
  BrowseAllow from @IF(name)
- 설명

BrowseAllow 는 열람파케트를 접수할수 있는 체계나 망을 지정합니다. 기정값은 **all** 입니다.

- **BrowseDeny**
  - 실례

    BrowseDeny from all
    BrowseDeny from none
    BrowseDeny from 192.0.2
    BrowseDeny from 192.0.2.0/24
    BrowseDeny from 192.0.2.0/255.255.255.0
    BrowseDeny from *.domain.com
    BrowseDeny from @LOCAL
    BrowseDeny from @IF(name)
  - 설명

BrowseDeny 는 열람파케트를 거부할 체계나 망을 지정합니다. 기정값은 **all** 입니다.

- **BrowseOrder**
  - 실례

    BrowseOrder allow,deny
    BrowseOrder deny,allow
  - 설명

BrowseOrder 는 **allow/deny** 처리순서를 지정합니다. 기정순서는 **deny,allow** 입니다:

  - **allow,deny** - 기정으로 열람파케트들을 거부하고 **BrowseDeny** 행 다음에 오는 **BrowseAllow** 행을 검사합니다.
  - **deny,allow** - 기정으로 열람파케트들을 허가하고 **BrowseAllow** 다음에 오는 **BrowseDeny** 행을 검사합니다.

- **BrowsePort**
  - 실례

    BrowsePort 631
    BrowsePort 9999

○ 설명

BrowsePort 는 열람파케트들이 리용하는 UDP 포구를 지정합니다. 기정값은 631 입니다. **BrowsePort** 를 열람하려고 하는 모든 체계들에서 같은 값을 설정해야 합니다.

- **BrowseProtocols**
  - 실례

    BrowseProtocols all
    BrowseProtocols none
    BrowseProtocols cups
    BrowseProtocols dnssd
    BrowseProtocols ldap
    BrowseProtocols lpd
    BrowseProtocols slp
    BrowseProtocols smb
    BrowseProtocols cups dnssd

  - 설명

BrowseProtocols 는 공유된 인쇄기를 국부망상에 공개하고 보여주기 위해 리용할 규약을 지정합니다. 공백으로 구분하여 여러개의 규약을 지정할수 있습니다. 기정규약은 **BrowseLocalProtocols** 에 대해서는 **CUPS dnssd** 이며 **BrowseRemoteProtocols** 에 대해서는 **CUPS** 입니다.

SLP 규약을 리용할 때 망에 한개 이상의 등록부대행체봉사기(DA)가 있어야 합니다. 다시 말하면 CUPS 는 망을 선택하는 몇초동안 의뢰기의 요청에 응답하지 않습니다.

BrowseRemoteProtocols

- 실례

  BrowseRemoteProtocols all
  BrowseRemoteProtocols none
  BrowseRemoteProtocols cups
  BrowseRemoteProtocols ldap
  BrowseRemoteProtocols slp

- 설명

BrowseRemoteProtocols 은 망상에서 원격공유인쇄기를 찾을 때 리용할 규약들을 지정합니다. 공백으로 구분하여 여러개의 규약을 지정할수 있습니다. 기정값은 **cups** 입니다.

- **BrowseShortNames**
  - 실례

    BrowseShortNames Yes
    BrowseShortNames No

  - 설명

BrowseShortNames 는 원격인쇄기에 대해 짧은 이름을 리용하겠는가를 지정합니다. 짧은 이름은 원격인쇄기이름입니다. 같은 이름으로 하나 이상의 원격인쇄기가 검출되면 인쇄기들은 긴 이름을 가지게 됩니다. 이 선택항목의 기정값은 **Yes** 입니다.

- **BrowseTimeout**
  - 실례

    BrowseTimeout 300
    BrowseTimeout 60
  - 설명

BrowseTimeout 열람파케트로부터 수신할 인쇄기나 클라스정보에 대한 중단시간을 설정합니다. 인쇄기나 클라스가 중단되면 목적지목록에서 삭제됩니다.

BrowseTimeout 값은 항상 **BrowseInterval** 값보다 커야 합니다.

- **BrowseWebIF**
  - 실례

    BrowseWebIF On
    BrowseWebIF Off
  - 설명

BrowseWebIF 는 CUPS 웨브대면부를 DNS-SD 를 통하여 공개하겠는가를 결정합니다. 기정값은 Off 입니다.

- **Browsing**
  - 실례

    Browsing On
    Browsing Off
  - 설명

Browsing 은 망인쇄열람을 할수 있도록 하겠는가를 결정합니다. 기정값은 **Yes** 입니다.

이 명령은 자체로 인쇄기를 공유하지 못합니다. 다른 체계에 국부인쇄기를 공개하려면 **BrowseAddress** 나 **BrowseProtocols** 명령을 리용해야 합니다.

- **DataDir**
  - 실례

    DataDir /usr/share/cups
  - 설명

DataDir 는 자료화일을 리용할 등록부를 지정합니다.

- **DefaultAuthType**
  - 실례

DefaultAuthType Basic
DefaultAuthType BasicDigest
DefaultAuthType Digest
DefaultAuthType Negotiate

- 설명

사용자이름을 요구하는 IPP 조작에 리용할 인증형태를 지정합니다. 기정값은 **Basic** 입니다.

- **DefaultCharset**
  - 실례

DefaultCharset utf-8
DefaultCharset iso-8859-1
DefaultCharset windows-1251

- 설명

DefaultCharset 는 의뢰기련결에 리용할 기정문자모임을 설정합니다. 기정문자모임은 **utf-8** 이지만 의뢰기나 **DefaultLanguage** 명령이 지정한 언어에 해당한 문자모임으로 재정의할수 있습니다.

- **DefaultShared**
  - 실례

DefaultShared yes
DefaultShared no

- 설명

DefaultShared 는 인쇄기를 기정으로 공유하겠는가를 지정합니다. 기정값은 **Yes** 입니다.

- **Deny**
  - 실례

```
<Location /path>
..
Deny from All
Deny from None
Deny from *.domain.com
Deny from .domain.com
Deny from host.domain.com
Deny from nnn.*
Deny from nnn.nnn.*
Deny from nnn.nnn.nnn.*
Deny from nnn.nnn.nnn.nnn
Deny from nnn.nnn.nnn.nnn/mm
Deny from nnn.nnn.nnn.nnn/mmm.mmm.mmm.mmm
Deny from xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx
Deny from @LOCAL
Deny from @IF(name)
```

</Location>

- 설명

Deny 는 봉사기에 대한 접근을 거부할 콤퓨터이름, IP 주소와 망이름을 지정합니다.

HostNameLookups 에 지정한 주콤퓨터이름과 령역이름만 허용됩니다 .

Deny 은 **Location** 나 **Limit** 내에 있어야 합니다.

- **DocumentRoot**
  - 실례

DocumentRoot /usr/share/doc/cups
DocumentRoot /foo/bar/doc/cups

- 설명

DocumentRoot 는 CUPS 에서 HTTP 봉사기의 웨브내용위치를 지정합니다. 절대경로를 지정하지 않으면 **ServerRoot** 등록부를 기준으로 상대경로라고 인정합니다. 기정등록부는 /usr/share/cups/www 입니다.

- **ErrorLog**
  - 실례

ErrorLog /var/log/cups/error_log
ErrorLog /var/log/cups/error_log-%s
ErrorLog syslog

- 설명

ErrorLog 는 오유기록화일이름을 설정합니다.

- **FontPath**
  - 실례

FontPath /foo/bar/fonts
FontPath /usr/share/cups/fonts:/foo/bar/fonts

- 설명

FontPath 는 서체경로를 탐색할 때 리용할 서체경로를 지정합니다. 기정서체경로는 /usr/share/cups/fonts 입니다.

- **Limit**
  - 실례

```
<Location /path>
 <Limit GET POST>
 ...
 </Limit>

 <Limit ALL>
 ...
 </Limit>
```

```
</Location>

<Policy name>
<Limit CUPS-Add-Modify-Printer CUPS-Delete-Printer>
...
</Limit>

<Limit All>
...
</Limit>
</Policy>
```

○ 설명

Limit 는 특정한 HTTP 요청형태에 대한 접근조종명령들을 배합합니다. 이 명령은 **Location** 나 **Policy** 내에 있어야 합니다. 접근은 개별적인 요청형태들(DELETE, GET, HEAD, OPTIONS, POST, PUT 와 TRACE)이나 모든 요청형태들(ALL)에 적용됩니다. 요청형태이름은 Apache 와의 호환성을 위해 경우에 따라 변동됩니다.

Policy 내에 포함되면 **Limit** 는 특정한 IPP 조작을 위해 접근조종명령들을 배합합니다. 공백으로 구분하여 여러가지 명령을 리용할수 있습니다. 표 8 에서 제공되는 조작들을 보여줍니다.

표 9. 제공되는 IPP 조작들

조작이름	설명
All	모든 조작들 - 목록에 포함되지 않은 조작들에 대해서도 기정제한을 적용할 때 리용
Cancel-Job	일감을 최소
Cancel-Subscription	서명을 취소
Create-Job	새로운 빈 일감창조
Create-Job-Subscription	일감에 대한 통보서명창조
Create-Printer-Subscription	인쇄기에 대한 통보서명창조
CUPS-Accept-Jobs	인쇄기에 대한 printer-is-accepting-jobs value 값을 true 로 설정
CUPS-Add-Modify-Class	부류를 추가하거나 변경
CUPS-Add-Modify-Printer	인쇄기를 추가하거나 변경
CUPS-Authenticate-Job	인쇄기일감인증
CUPS-Delete-Class	부류삭제
CUPS-Delete-Printer	인쇄기삭제

CUPS-Get-Classes	부류목록얻기
CUPS-Get-Default	(망/봉사기)기정인쇄기나 부류얻기
CUPS-Get-Devices	리용할수 있는 장치목록얻기
CUPS-Get-PPDs	가능한 구동쏘프트웨어얻기
CUPS-Get-Printers	인쇄기나 부류목록얻기
CUPS-Move-Job	일감을 다른곳으로 이전
CUPS-Reject-Jobs	printer-is-accepting-jobs 값을 false 로 설정
CUPS-Set-Default	망/봉사기기정인쇄기설정
Disable-Printer	printer-state 변수를 stopped 로 설정
Enable-Printer	printer-state 를 idle/processing 로 설정
Get-Job-Attributes	일감정보얻기
Get-Jobs	일감목록얻기
Get-Notifications	사건목록얻기
Get-Printer-Attributes	인쇄기정보얻기
Get-Subscription-Attributes	서명정보얻기
Get-Subscriptions	서명목록얻기
Hold-Job	일감선택
Pause-Printer	printer-state 값을 stopped 로 설정
Print-Job	한개 화일로 일감창조
Purge-Jobs	인쇄기의 모든 일감을 삭제
Release-Job	이전 일감을 해방
Renew-Subscription	서명을 새로작성
Restart-Job	일감을 다시 인쇄
Resume-Printer	printer-stae 값을 idle/processing 로 설정
Send-Document	Create-Job 로 창조한 일감에 화일을 추가
Set-Job-Attributes	일감선택항목변경
Validate-Job	일감유효성검사

- **Listen**
  - 실례

    Listen 127.0.0.1:631
    Listen 192.0.2.1:631
    Listen [::1]:631
    Listen *:631
  - 설명

Listen 은 련결을 청취할 망주소와 포구를 지정합니다.

Listen 은 **Port** 명령과 류사한데 특수한 대면부나 망에 대한 접근을 제한합니다.

- **Location**
  - 실례

    <Location 봉사기위치>
    ...
    </Location>
  - 설명

Location 은 특정한 HTTP 자원이나 경로에 대한 접근조종 및 인증선택항목을 설정합니다. **Allow**, **AuthType**, **Deny**, **Encryption**, **Limit**, **LimitExcept**, **Order**, **Require** 와 **Satisfy** 는 모두 하나의 **location** 내에 있어야 합니다.

표 10. 봉사기의 위치

위치	설명
/	모든 get 조작에 대한 경로(get-printers, get-jobs)
/admin	모든 관리조작에 대한 경로(add-printer, delete-printer, start-printer)
/admin/conf	CUPS 구성화일에 대한 접근경로(cupsd.conf, client.conf)
/admin/log	CUPS 작업기록화일에 대한 접근경로(access_log, error_log, page_log)
/classes	모든 부류에 대한 경로
/classes/name	부류의 이름에 대한 자원
/jobs	모든 일감에 대한 경로(hold-job, release-job)
/jobs/id	일감식별자에 대한 자원
/printers	모든 인쇄기들에 대한 경로
/printers/name	인쇄기이름경로
/printers/name.ppd	인쇄기이름에 해당한 PPD 화일경로

- **LogLevel**
  - 실례

    LogLevel none
    LogLevel emerg
  - 설명

LogLevel 은 **ErrorLog** 화일에 기록할 준위를 지정합니다. 준위에는 다음과 같은 값들이 있습니다:

- none - 아무것도 기록하지 않음
- emerg - 봉사기실행을 방해하는 긴급조건을 기록
- alert - 긴급조종되여야 하는 통보기록

- crit - 봉사기실행에 영향을 주는 치명적오유를 기록
- error - 일반오유기록
- warn - 오유 및 경고들을 기록
- notice - 림시화일오유조건을 기록
- info - 모든 요청들과 변경상태를 기록
- debug - 기본오유추적정보를 기록
- debug2 - 모든 오유추적정보를 기록

기정 **LogLevel** 값은 **warn** 입니다.

- **LogTimeFormat**
  - 실례

    LogTimeFormat standard
    LogTimeFormat usecs
  - 설명

LogTimeFormat 는 기록화일에 기록되는 날자와 시간형식을 지정합니다. **Standard** 는 표준 Apache 기록형식의 날자와 usecs 의 시간형식을 리용합니다. 기정값은 **standard** 입니다.

- **MaxJobs**
  - 실례

    MaxJobs 100
    MaxJobs 9999
    MaxJobs 0
  - 설명

MaxJobs 는 기억기에 유지할 최대일감수를 지정합니다. 일감의 수가 한계값에 도달하면 제일 마지막에 완성된 일감은 체계에서 삭제되고 새로운 일감의 대기렬위치를 결정합니다. 현재 모든 일감이 처리중에 있다면 새로운 일감은 배제됩니다.

최대값을 0 으로 설정하면 이 기능을 사용할수 없습니다. 기정설정값은 500 입니다.

- **Order**
  - 실례

    <Location /path>
    ...
    Order Allow,Deny
    Order Deny,Allow
    </Location>
  - 설명

Order 는 기정접근조조을 정의합니다. 다음의 값들이 지원됩니다:

- **allow,deny** - 기정으로 요청을 거부하고 다음 **Deny** 행 다음에 있는 Allow 행을 검사합니다.
- **deny,allow** - 기정으로 요청을 허가하고 다음 **Allow** 행 다음에 있는 **Deny** 행을 검사합니다.

Order 는 **Location** 나 **Limit** 내에 있어야 합니다.

- **Policy**
  - 실례

<Policy name>
<Limit operation ... operation>
...
</Limit>
<Limit operation ... operation>
...
</Limit>
<Limit All>
...
</Limit>
</Policy>

  - 설명

Policy 에 IPP 조작접근한계를 지정합니다. 매 정책은 특정조작들-사용자한계, 인증, 암호화, 허가/거부할 주소, 령역과 주콤퓨터에 대한 접근조종한계를 설정합니다. <Limit All>는 모든 조작들에 대한 접근조종제한을 명시합니다.

- **Port**
  - 실례

Port 631
Port 80

  - 설명

Port 에 청취할 포구를 지정합니다. 기정포구는 631 입니다.

- **RemoteRoot**
  - 실례

RemoteRoot remroot
RemoteRoot root

  - 설명

RemoteRoot 에 원격콤퓨터로부터 들어오는 인증하지 않는 사용자이름을 설정합니다. 기정사용자이름은 **remroot** 입니다. **RemoteRoot** 를 **root** 로 설정하면 이 보안기능은 무시됩니다.

- **RequestRoot**

- 실례
  RequestRoot /var/spool/cups
  RequestRoot /foo/bar/spool/cups
- 설명

RequestRoot 에 IPP 요청과 HTML 을 위한 등록부를 설정합니다. 절대경로를 지정하지 않으면 **ServerRoot** 등록부로부터 상대경로로 합니다. 기정요청등록부는 /var/spool/cups 입니다.

- **Require**
  - 실례
    <Location /path>
    ...
    Require group foo bar
    Require user john mary
    Require valid-user
    Require user @groupname
    Require user @SYSTEM
    Require user @OWNER
    </Location>
  - 설명

Require 는 자원에 대하여 인증하겠는가를 지정합니다. 인증될 사용자는 **group** 뒤에 오는 하나이상의 집단성원이여야 합니다.

user 는 인증될 사용자가 **user** 뒤에 오는 사용자들중 하나이거나 집단의 성원이여야 한다는것을 지정합니다. 집단이름은 앞붙이 @를 붙입니다.

valid-user 는 인증될 사용자가 자원에 접근할수 있다는것을 표시합니다.

기정값은 인증을 하지 않는것입니다. 이 명령은 **Location** 이나 **Limit** 내에 있어야 합니다.

- **ServerBin**
  - 실례
    ServerBin /usr/lib/cups
    ServerBin /foo/bar/lib/cups
  - 설명

ServerBin 에 봉사기가 리용하는 실행가능한 화일들의 등록부를 설정합니다. 절대경로를 지정하지 않으면 **ServerRoot** 등록부로터 상대경로 인식합니다. 기정실행화일등록부는 /usr/lib/cups, /usr/lib32/cups 와 /usr/libexec/cups 입니다.

- **ServerName**
  - 실례
    ServerName foo.domain.com
    ServerName myserver.domain.com
  - 설명

ServerName 에 의뢰기에 보고할 주콤퓨터이름을 지적합니다. 기정으로는 봉사기이름이 주콤퓨터이름입니다.

- **ServerRoot**
  - 실례

    ServerRoot /etc/cups
    ServerRoot /foo/bar/cups
  - 설명

ServerRoot 에 봉사기구성 및 상태화일들에 대한 절대경로를 지정합니다. 또한 cupsd.conf 에서 상대경로로 리용합니다. 기정봉사기등록부는 */etc/cups* 입니다.

- **User**
  - 실례

    User lp
    User guest
  - 설명

User 에 려과기와 CGI 쏘프트웨어를 실행할 Unix 체계사용자들을 설정합니다. 기정사용자는 lp 입니다. 체계의 보안위험성이 로출될수 있으므로 사용자 root 는 사용하지 말아야 합니다. 식별자가 0 인 사용자를 지정하면 자동적으로 **nobody** 가 선택될것입니다.

3) 인쇄봉사기의 시작

《붉은별》 봉사기용체계 3.0 을 설치하면 /etc/cups/cupsd.conf 화일에 기정항목들이 이미 설정됩니다.

설정된 값들은 다음과 같습니다.

```
MaxLogSize 0
LogLevel warn
SystemGroup sys root
# Allow remote access
Port 631
Listen /var/run/cups/cups.sock
# Show shared printers on the local network.
Browsing On
BrowseOrder allow,deny
BrowseAllow all
BrowseRemoteProtocols CUPS smb
BrowseAddress @LOCAL
BrowseLocalProtocols CUPS dnssd
DefaultAuthType Basic
<Location />
 Order allow,deny
```

```
 Allow all
</Location>
<Location /admin>
 Order allow,deny
 Allow all
</Location>
<Location /admin/conf>
 AuthType Default
 Require user @SYSTEM
 Order allow,deny
 Allow all
</Location>
<Policy default>
 <Limit Send-Document Send-URI Hold-Job Release-Job Restart-Job Purge-Jobs Set-Job-Attributes Create-Job-Subscription Renew-Subscription Cancel-Subscription Get-Notifications Reprocess-Job Cancel-Current-Job Suspend-Current-Job Resume-Job CUPS-Move-Job CUPS-Get-Document>
 Require user @OWNER @SYSTEM
 Order deny,allow
 Allow from all
 </Limit>
 <Limit CUPS-Add-Modify-Printer CUPS-Delete-Printer CUPS-Add-Modify-Class CUPS-Delete-Class CUPS-Set-Default CUPS-Get-Devices>
 AuthType Default
 Require user @SYSTEM
 Order deny,allow
 Allow from all
 </Limit>
 <Limit Pause-Printer Resume-Printer Enable-Printer Disable-Printer Pause-Printer-After-Current-Job Hold-New-Jobs Release-Held-New-Jobs Deactivate-Printer Activate-Printer Restart-Printer Shutdown-Printer Startup-Printer Promote-Job Schedule-Job-After CUPS-Accept-Jobs CUPS-Reject-Jobs>
 AuthType Default
 Require user @SYSTEM
 Order deny,allow
 Allow from all
 </Limit>
 <Limit Cancel-Job CUPS-Authenticate-Job>
 Require user @OWNER @SYSTEM
 Order deny,allow
 Allow from all
 </Limit>
 <Limit All>
 Order deny,allow
 Allow from all
 </Limit>
</Policy>
<Policy authenticated>
 <Limit Create-Job Print-Job Print-URI>
```

```
    AuthType Default
    Order deny,allow
    Allow from all
    </Limit>

    <Limit Send-Document Send-URI Hold-Job Release-Job Restart-Job Purge-Jobs Set-Job-Attributes Create-Job-Subscription Renew-Subscription Cancel-Subscription Get-Notifications Reprocess-Job Cancel-Current-Job Suspend-Current-Job Resume-Job CUPS-Move-Job CUPS-Get-Document>
    AuthType Default
    Require user @OWNER @SYSTEM
    Order deny,allow
    Allow from all
    </Limit>
    <Limit CUPS-Add-Modify-Printer CUPS-Delete-Printer CUPS-Add-Modify-Class CUPS-Delete-Class CUPS-Set-Default>
    AuthType Default
    Require user @SYSTEM
    Order deny,allow
    Allow from all
    </Limit>
    <Limit Pause-Printer Resume-Printer Enable-Printer Disable-Printer Pause-Printer-After-Current-Job Hold-New-Jobs Release-Held-New-Jobs Deactivate-Printer Activate-Printer Restart-Printer Shutdown-Printer Startup-Printer Promote-Job Schedule-Job-After CUPS-Accept-Jobs CUPS-Reject-Jobs>
    AuthType Default
    Require user @SYSTEM
    Order deny,allow
    Allow from all
    </Limit>
    <Limit Cancel-Job CUPS-Authenticate-Job>
    AuthType Default
    Require user @OWNER @SYSTEM
    Order deny,allow
    Allow from all
    </Limit>
    <Limit All>
    Order deny,allow
    Allow from all
    </Limit>
   </Policy>
    BrowseWebIF Yes
```

다음의 지령을 실행하여 인쇄봉사기대몬을 시작합니다.

```
#service  cups start
```

인쇄봉사기가 정상적으로 시작하면 이 봉사기에 접속된 인쇄기들을 관리할 수 있게 됩니다.

이 사용지도서에서는 인쇄봉사기에 USB 포구를 리용하여 국부적으로 접속된 인쇄기를 관리하면서 인쇄하는 방법을 설명합니다.

4) 인쇄봉사기로의 접속

말단의뢰기들에서 리용하는 웨브열람기에서 다음의 주소에 접속합니다.

https://봉사기주소:631

여기서 봉사기주소는 인쇄봉사기쏘프트웨어를 설치한 봉사기의 주소입니다.

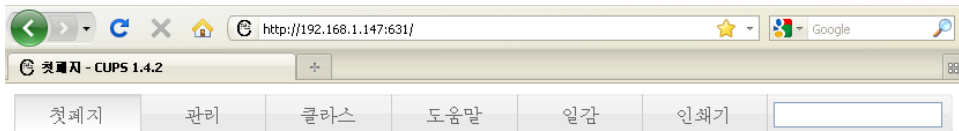



그림 32. 인쇄봉사기관리페지의 첫화면

인쇄봉사기가 정상동작하고있다면 웨브열람기에는 우의 그림과 같은 인쇄봉사기관리페지화면이 현시됩니다.

인쇄봉사기관리페지는 6개의 표쪽들로 이루어져 있습니다.

우의 그림에서 보여주는 페지가 인쇄봉사기관리페지의 첫번째 표쪽인 **첫페지**표쪽입니다. 여기에서는 인쇄봉사기의 개념과 리용방법들을 소개합니다.

두번째표쪽인 **관리**표쪽은 인쇄기의 추가, 검색 및 삭제와 같은 인쇄기관리기능과 함께 클라스관리기능, 일감관리기능, 기타 봉사기의 구성설정기능을 수행할수 있습니다. 아래의 그림에서 **관리**표쪽화면을 보여줍니다.

그림 33. 인쇄봉사기관리페지의 관리표쪽화면

이외에도 **클라스**, **일감**, **인쇄기**관리표쪽들과 도움말정보들을 현시하는 **도움말**표쪽들이 있습니다.

5) 인쇄봉사기의 관리

인쇄봉사기관리페지에서 두번째 표쪽인 **관리**표쪽에서는 인쇄기의 추가 및 검색기능과 클라스의 추가기능, 인쇄봉사기의 기본설정변경, 기록정보의 보기기능을 수행합니다.

인쇄봉사기를 관리하기 위한 대부분의 작업들은 모두 사용자인증을 요구합니다. 사용자인증창문이 펼쳐지며 인쇄봉사기를 리용하려는 사용자의 이름과 통과암호를 입력하여 인쇄봉사기를 관리하기 위한 사용자인증정보를 확인하여야 합니다.

(1) 인쇄기의 추가

인쇄봉사기를 리용하기 위한 첫작업은 새로운 인쇄기를 추가하는 작업입니다.

인쇄기를 추가하려면 **관리**표쪽페지에서 **인쇄기추가단추**를 리용할수 있습니다. 또는 **새 인쇄기탐색**단추를 리용하여 자동적으로 검색한 인쇄기를 추가할수도 있습니다.

여기서 **인쇄기추가**단추를 누르면 먼저 추가할수 있는 인쇄기들을 검색하며 검색결과화면이 펼쳐집니다.

그림 34. 인쇄기검색화면

검색결과는 **국부인쇄기**와 **탐색된 망인쇄기**, **기타 망인쇄기**로 구분하여 《인쇄기류형(인쇄기자호)》의 형식으로 목록으로 현시됩니다. 여기에서 인쇄기자호가 **알수 없음**이 아닌 항목이 실지 봉사기에 련결되여있는 인쇄기입니다. 우의 그림은 인쇄봉사기에 직렬포구로 자호가 《HP DeskJet 3538》인 인쇄기를 련결한 상태에서 인쇄기추가단추를 눌렀을 때 현시되는 인쇄기검색결과화면입니다.

국부인쇄기 hp deskjet 3500 (hp deskjet 3500)를 선택하고 **계속하기**단추를 누르면 아래의 그림에서 보여주는것과 같은 화면이 현시됩니다.

그림 35. 인쇄기이름설정

여기에서 접속된 인쇄기를 선택할 때 리용하는 이름을 《hp_deskjet_3500》으로 입력합니다. 또한 이 인쇄기를 말단사용자들도 리용할수 있도록 공유하기 위하여 아래부분의 검사항목을 선택합니다.

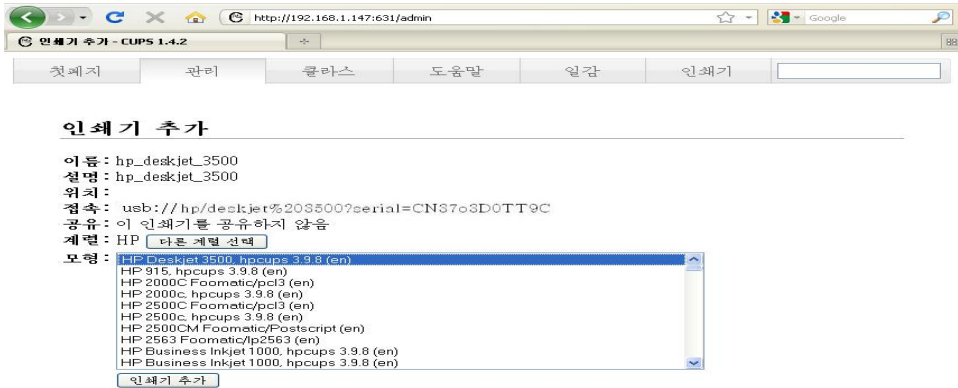



그림 36. 인쇄기의 계렬과 모형선택

인쇄기가 자기의 장치구동쏘프트웨어를 정확히 찾는다면 우의 그림에서와 같이 인쇄기의 계렬과 모형이 이미 선택된 상태로 되여있으며 장치구동쏘프트웨어를 찾지 못한 경우에는 수동으로 선택하여야 합니다. 이와 같은 경우는 대부분이 해당한 인쇄기의 구동쏘프트웨어를 설치하지 않은 경우이며 이때는 자기의 구동쏘프트웨어를 따로 설치해주어야 합니다.

인쇄기의 계렬과 모형을 정확히 선택하였다면 **인쇄기추가**단추를 누릅니다.

《hp_deskjet_3500》이라는 이름을 가진 인쇄기가 추가되고 이 인쇄기의 구성항목들을 설정하는 창문이 현시됩니다.

필요한 구성항목들을 설정하고 **구성항목의 설정**단추를 누르면 성과적으로 설정하였다는 통보문이 현시된 다음 아래의 그림에서 보여주는 인쇄기관리화면이 현시됩니다.

http://192.168.1.147:631/printers/hp_deskjet_3500

hp_deskjet_3500 - CUPS 1.4.2

첫페지 | 관리 | 클라스 | 도움말 | 일감 | 인쇄기

hp_deskjet_3500 (대기중, 일감을 접수중, 공유되지 않음)

정비 | 관리

설명 : hp_deskjet_3500
위치 :
인쇄기구동기 : HP Deskjet 3500, hpcups 3.9.8 (색)
접속대상 : usb://hp/deskjet%203500?serial=CN37o3D0TT9C
기정설정 : 상징폐지=없음 용지크기=iso_a4_210x297mm

일감

hp_deskjet_3500에서 검색 : 검색 지우기

수행된 일감 표시 | 모든 일감 표시

일감이 없습니다.

그림 37. 인쇄기 hp_deskjet_3500 의 관리화면

(2) 새 인쇄기의 탐색

봉사기에 설치되여있는 새로운 인쇄기를 검색하려면 **관리**표쪽에서 **새 인쇄기탐색**단추를 누릅니다. 인쇄봉사기는 아래의 그림에서와 같이 사용가능한 인쇄기들의 목록을 현시합니다.

해당한 인쇄기의 앞에 있는 **인쇄기추가**단추를 누르면 앞에서 진행한 인쇄기의 추가방식대로 새로운 인쇄기를 추가할수 있습니다.

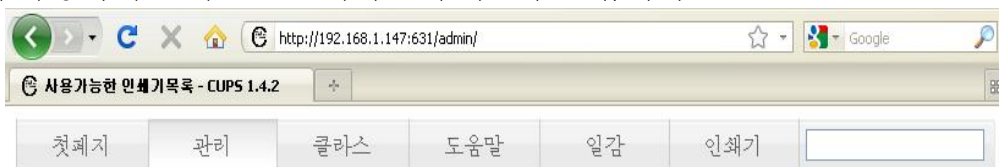



그림 38. 사용가능한 인쇄기목록현시

(3) 클라스의 추가

봉사기에 설치되여있는 여러개이 인쇄기들을 묶어서 하나의 클라스로 리용할수도 있습니다.

그림 39. 클라스의 추가

인쇄기들의 묶음인 클라스를 추가하려면 **관리**표쪽에서 **클라스추가**단추를 누릅니다. 우의 그림에서와 같이 클라스추가화면이 현시됩니다.

먼저 클라스의 이름을 class1 라고 입력하고 성원목록에서 하나이상의 인쇄기들을 선택합니다. 다음 **클라스추가**단추를 누르면 새로운 클라스가 추가되면서 아래의 그림에서와 같이 이름이 class1 인 클라스의 관리화면이 현시됩니다.

http://192.168.1.147:631/classes/class1

class1 - CUPS 1.4.2

첫페지 관리 클라스 도움말 일감 인쇄기

class1 (대기중, 일감접수중, 공유됨)

정비 관리

설명：

위치：

성원：hp_deskjet_3500

기정：상징페지=없음 매체=알수없음

일감

class1에서 검색： 검색 지우기

수행된 일감 표시 모든 일감 표시

일감이 없습니다.

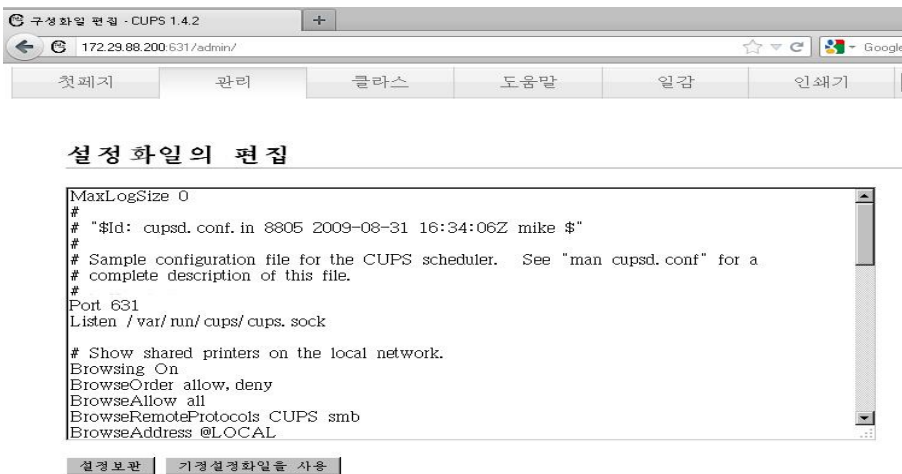
그림 40. 클라스 class1 의 관리화면

(4) 봉사기의 설정

인쇄봉사기의 구성항목들은 /etc/cups/cupsd.conf 화일에 등록됩니다. 이 구성화일을 수정하여 인쇄봉사기들의 설정을 변경시킬수 있습니다.

구성화일은 인쇄봉사기관리페지의 **관리**표쪽에서 **설정화일의 편집**단추를 리용하여 편집할수 있습니다.

설정화일의 편집단추를 누르면 구성화일의 내용을 편집할수 있는 편집창이 펼쳐집니다. 여기에서 필요한 내용들을 수정할수 있으며 또는 **기정설정화일을 사용**단추를 리용하여 기정설정화일의 내용으로 바꿀수도 있습니다. 해당한 내용을 수정한 다음 **설정보관**단추를 눌러 편집된 내용을 보관합니다. 그러면 해당한 설정에 맞게 인쇄봉사기를 재시작합니다.

그림 41. 설정화일의 편집

인쇄봉사기의 구성화일은 또한 **봉사기설정:**마당에서의 검사단추를 리용하여 변경시킬수도 있습니다.

관리표쪽의 오른쪽에는 인쇄봉사기의 구성정보를 변경시킬수 있는 여러가지 검사항목들이 있습니다. **상세설정**을 리용하여 보다 상세한 검사항목들을 리용할수 있습니다. 필요한 검사항목들을 선택 또는 선택해제한 다음 **설정의 변경**단추를 누르면 해당한 구성정보들을 리용하여 인쇄봉사기를 재시작합니다

(5) 기록정보 보기

봉사기관리페지의 **관리**표쪽에서는 **접근기록보기**, **오유기록보기**, **페지기록보기**단추를 리용하여 인쇄봉사기의 동작상태를 보여주는 기록정보들을 현시할수 있습니다.

6) 인쇄기 관리

봉사기관리페지의 **관리**표쪽에서 **인쇄기관리**단추를 누르던가 또는 **인쇄기** 표쪽을 펼치면 아래의 그림과 같이 인쇄봉사기에 등록되여있는 인쇄기들의 목록을 현시하는 화면이 펼쳐집니다.

그림 42. 인쇄기목록

웃부분에 있는 본문편집칸에 인쇄기의 이름문자렬을 입력하고 **검색**단추를 누르면 그 문자렬을 포함한 인쇄기들의 목록을 검색합니다.

인쇄기목록의 **인쇄기이름**렬에서 해당한 인쇄기를 누르면 아래의 그림과 같이 그 인쇄기를 관리하는 창문이 현시됩니다.

그림 43. 인쇄기관리

인쇄기관리화면에서 맨 웃부분에는 인쇄기관리와 관련한 2개의 조합칸이 있습니다. 그 아래에 인쇄기의 설정정보들을 보여주는 설정정보현시부가 있으며 아래부분에는 인쇄기에 등록되여있는 일감들을 보여주는 일감부분이

있습니다. 이 일감부분에서는 현재 인쇄기가 처리해야 하는 활성일감들의 목록을 보여주며 **수행된 일감표시, 모든 일감표시**단추를 리용하여 이미 수행된 일감들의 목록만을 보여주거나 또는 모든 일감들을 다 현시하게 할수 있습니다.

(1) 인쇄기의 변경

인쇄기관리화면에서 왼쪽조합칸에서는 **정비**를 선택하고 오른쪽조합칸에서 **인쇄기의 변경**을 선택하면 새로운 인쇄기류형을 검색하는 동작으로부터 시작하여 인쇄기추가와 같은 방법으로 현재 인쇄기를 변경할수 있습니다.

(2) 인쇄기의 삭제

인쇄기관리화면에서 왼쪽조합칸에서는 **정비**를 선택하고 오른쪽조합칸에서 **인쇄기의 삭제**를 선택하면 현재 인쇄기가 인쇄기목록에서 삭제됩니다.

(3) 인쇄기의 설정과 변경

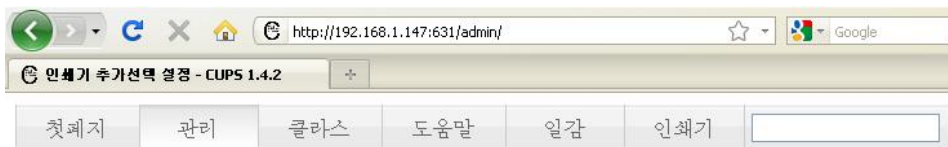



그림 44. 인쇄기의 구성항목(일반)의 변경

인쇄기관리화면에서 왼쪽조합칸에서는 **정비**를 선택하고 오른쪽조합칸에서 **인쇄기의 설정의 변경**을 선택하면 우의 그림과 같이 현재 인쇄기의 구성항목들을 변경하기 위한 페지가 현시됩니다.

이 페지에서는 **일반**구성항목들을 설정할수 있고 **설치된** 추가선택들에 대한 관리, **상징페지**의 추가관리, **방책**관리와 관련한 구성항목들을 변경할수 있습

니다. 해당한 구성항목들을 변경한 다음 **구성항목의 설정**단추를 누르면 변경된 구성정보들이 적용됩니다.

(4) 기정인쇄기로 설정

인쇄기관리화면에서 왼쪽조합칸에서는 **정비**를 선택하고 오른쪽조합칸에서 **기정인쇄기로 설정**을 선택하면 현재 인쇄기를 봉사기의 기정인쇄기로 설정합니다.

(5) 허가하는 사용자의 설정

인쇄기관리화면에서 왼쪽조합칸에서는 **정비**를 선택하고 오른쪽조합칸에서 **허가하는 사용자의 설정**을 선택하면 아래의 그림과 같이 현재 인쇄기의 사용을 허가 또는 금지하는 사용자들을 등록하기 위한 페지가 현시됩니다.

본문칸에 사용자의 이름을 입력하고 **인쇄허가** 또는 **인쇄금지**를 선택한 다음 **설정**단추를 누르면 인쇄기를 허가/금지하려는 사용자들이 등록됩니다.

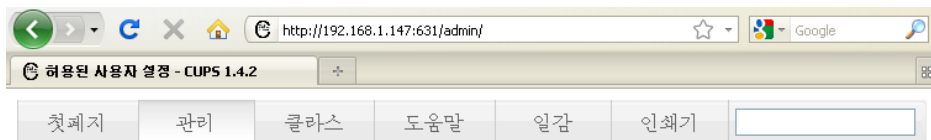



그림 45. 인쇄기사용을 허가/금지하는 사용자의 설정

(6) 시험페지의 인쇄

인쇄기관리화면의 왼쪽조합칸에서 **시험페지의 인쇄**를 선택하면 인쇄기로 시험페지를 인쇄합니다.

(7) 인쇄기의 시작/중지

인쇄기관리화면의 왼쪽조합칸에서 **인쇄기의 중지**를 선택하면 현재 인쇄기를 중지합니다. 이 항목은 인쇄기가 이미 시작되여있을 때 보이는 항목이며 인쇄기를 중지시킨 다음에는 **인쇄기의 시작**이라는 항목으로 바뀌여집니다.

(8) 일감을 거부/접수

인쇄기관리화면의 왼쪽조합칸에서 **일감을 거부**를 선택하면 현재 인쇄기에로 들어오는 모든 일감들을 거부합니다. 인쇄기가 일감거부상태에 있는 경우에 이 항목은 **일감을 접수**라는 항목으로 바뀌며 이 항목을 선택하면 그 다음부터 인쇄기는 새로 들어오는 일감들을 거부하지 않습니다.

(9) **모든 일감을 이동**

인쇄기관리화면의 왼쪽조합칸에서 **모든 일감을 이동**을 선택하면 현재 활성화된 모든 일감들을 수행할 다른 인쇄기나 클라스를 선택하기 위한 새로운 목적지선택폐지가 현시되며 여기에서 목적지를 선택한 다음 **일감 이동**단추를 누르면 선택된 목적지에로 일감들이 이동합니다.

(10) 모든 일감을 취소

인쇄기관리화면의 왼쪽조합칸에서 **모든 일감을 취소를** 선택하면 현재 활성화된 모든 일감들을 취소합니다.

7) 일감관리

봉사기관리페지의 **관리**표쪽에서 **일감관리**단추를 누르던가 또는 **일감**표쪽을 펼치면 아래의 그림과 같이 인쇄봉사기에 등록되여있는 모든 활성화된 일감들의 목록을 현시하는 화면이 펼쳐집니다.

그림 46. 일감목록

여기에서 **수행된 일감표시, 모든 일감표시**단추를 눌러 현재 이미 수행된 일감들을 표시하거나 또는 모든 일감들을 표시할수 있습니다.

활성화된 일감목록에서는 **조종**렬에 **일감보류, 일감취소, 일감이동**단추가 있으며 이 단추들을 리용하여 해당한 일감을 보류시키거나 취소시킬수 있으며 다른 인쇄기나 클라스로 이동시킬수도 있습니다.

8) 클라스관리

봉사기관리페지의 **관리**표쪽에서 **클라스관리**단추를 누르던가 또는 **클라스**표쪽을 펼치면 아래의 그림과 같이 인쇄봉사기에 등록되여있는 클라스들의 목록을 현시하는 화면이 펼쳐집니다.

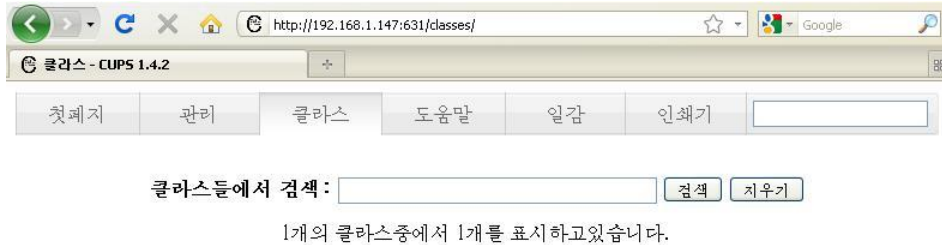



그림 47. 클라스목록

웃부분에 있는 본문편집칸에 이름의 부분문자렬을 입력하고 **검색**단추를 누르면 그 문자렬을 포함한 클라스들의 목록을 검색합니다.

그림 48. 클라스관리

검색된 클라스목록에서 **성원**렬은 그 클라스가 포함하고있는 인쇄기들을 반점으로 구분하여 보여주고있으며 매 인쇄기들을 누르면 그 인쇄기의 관리페지가 현시됩니다.

클라스이름렬에서 해당한 클라스를 누르면 우의 그림에서와 같이 클라스의 관리화면이 현시됩니다.

클라스관리화면에서 맨 웃부분에는 클라스관리와 관련한 2개의 조합칸이 있습니다. 그 아래에 클라스의 정보들을 현시하는 부분이 있으며 아래부분에는 클라스에 등록된 일감들을 보여주는 일감부분이 있습니다. 이 일감부분에서는 현재 클라스의 모든 성원인쇄기들이 처리해야 하는 활성일감들의 목록을 보여주며 **수행된 일감표시, 모든 일감표시**단추를 리용하여 이미 수행된 일감들의 목록만을 보여주거나 또는 모든 일감들을 다 현시하게 할수 있습니다.

(1) 클라스의 변경

클라스관리화면에서 왼쪽조합칸에서는 **정비**를 선택하고 오른쪽조합칸에서 클라스**의 변경**을 선택하면 클라스의 **설명**과 **위치**, **성원**들을 변경하는 기능을 수행할수 있는 아래의 그림과 같은 화면이 현시됩니다.

여기서 해당한 값들을 다시 설정하고 **변경**단추를 누르면 새로 설정된 값들로 클라스의 정보들이 변경됩니다.

그림 49. 클라스변경

(2) 클라스의 삭제

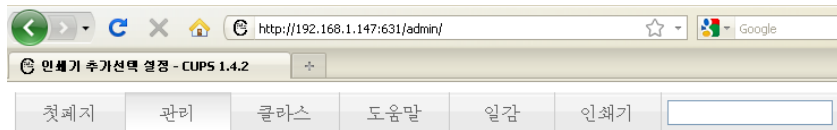
클라스관리화면에서 왼쪽조합칸에서는 **정비**를 선택하고 오른쪽조합칸에서 **클라스의 삭제**를 선택하면 현재 클라스가 목록에서 삭제됩니다.

(3) 클라스의 설정과 변경

클라스관리화면에서 왼쪽조합칸에서는 **정비**를 선택하고 오른쪽조합칸에서 **클라스의 설정의 변경**을 선택하면 아래의 그림과 같이 현재 클라스의 구성항목들을 변경하기 위한 페지가 현시됩니다.

http://192.168.1.147:631/admin/

인쇄기 추가선택 설정 - CUPS 1.4.2

첫페지 관리 클라스 도움말 일감 인쇄기

class1 의 구성항목 변경

상징페지 방책

상징페지

시작 상징페지 : none

끝 상징페지 : none

구성항목의 설정

그림 50. 클라스의 구성항목의 변경

이 페지에서는 **상징페지**의 추가관리, **방책**관리와 관련한 구성항목들을 변경할수 있습니다. 해당한 구성항목들을 변경한 다음 **구성항목의 설정**단추를 누르면 변경된 구성정보들이 적용됩니다.

(4) 기정클라스로 설정

클라스관리화면에서 왼쪽조합칸에서는 **정비**를 선택하고 오른쪽조합칸에서 **기정클라스로 설정**을 선택하면 현재 클라스를 봉사기의 기정클라스로 설정합니다.

(5) 허가하는 사용자의 설정

클라스관리화면에서 왼쪽조합칸에서는 **정비**를 선택하고 오른쪽조합칸에서 **허가하는 사용자의 설정**을 선택하면 현재 클라스의 사용을 허가 또는 금지하는 사용자들을 등록하기 위한 페지가 현시됩니다.

본문칸에 사용자의 이름을 입력하고 **인쇄허가** 또는 **인쇄금지**를 선택한 다음 **설정**단추를 누르면 클라스를 허가/금지하려는 사용자들이 등록됩니다.

(6) 클라스의 시작/중지

클라스관리화면의 왼쪽조합칸에서 **클라스의 중지**를 선택하면 현재 클라스를 중지합니다. 이 항목은 클라스가 이미 시작되여있을 때 보이는 항목이며 클라스를 중지시킨 다음에는 **클라스의 시작**이라는 항목으로 바뀌여집니다.

(7) 모든 일감을 이동

클라스관리화면의 왼쪽조합칸에서 **모든 일감을 이동**을 선택하면 현재 활성화된 모든 일감들을 수행할 다른 클라스나 클라스를 선택하기 위한 새로운 목

적지선택페지가 현시되며 여기에서 목적지를 선택한 다음 **일감 이동**단추를 누르면 선택된 목적지에로 일감들이 이동합니다.

(8) 모든 일감을 취소

클라스관리화면의 왼쪽조합칸에서 **모든 일감을 취소를** 선택하면 현재 활성화된 모든 일감들을 취소합니다.

(9) 인쇄봉사기의 중지

인쇄봉사기는 다음의 지령에 의하여 중지시킵니다.

```
#service  cups stop
```

제7장. 가상화환경

이 장에서는 가상화체계 1.0 에 대한 사용방법을 설명합니다.
《붉은별》 봉사기용체계 3.0 에서 여러개의 봉사기용체계를 동시에 가동시키는 환경을 제공합니다.

제1절. 개요

1. 목적

봉사기체계의 보안을 강화하고 봉사기대의 자원리용의 효률성을 높이기 위해서입니다.
가상화지원부는 한대의 봉사기대에 여러개의 《붉은별》 봉사기용체계 3.0 을 설치하여 리용할수 있게 합니다.

2. 화일목록

- 가상화서고
  libvirt-0.10.2-18
  libvirt-client-0.10.2-18
  libvirt-python-0.10.2-18
- 가상체계설치쏘프트웨어
  python-virtinst-0.600.0-15
- 완전가상화쏘프트웨어
  qemu-kvm-0.12.1.2-2.335
  qemu-img-0.12.1.2-2.335

3. 가동환경

－ 하드웨어환경
- RAM 1G 이상
- 하드용량 10GB 이상
- VT 기술을 갖춘 CPU 요구

－ 쏘프트웨어환경
- 조작체계

《붉은별》 봉사기용체계 3.0

4. 구성관계

－ 쏘프트웨어의 부분품들의 이름과 목적, 운영에 대한 개요

- qemu-img

가상체계용 영상화일의 설치쏘프트웨어

－ 쏘프트웨어의 부분품들의 성능특성들

- 쏘프트웨어가 만들어내는 출력물들의 류형, 크기, 속도

인수로 지정한 이름과 크기의 영상화일(.img)을 생성합니다.

표 11. 용어 및 략어

용 어	정 의
KVM(Kernel-based Virtual Machine)	핵심부기반의 가상기계로서 VT(가상화기술)을 갖춘 CPU 를 요구합니다.
주조작체계 (Host Operating System)	여러 가상조작체계들을 설치하고 관리하는 대몬이 있는 기본조작체계로서 유일합니다.
가상조작체계 (Guest Operating System)	주조작체계우에 설치하는 체계로서 여러개일수 있습니다.
GUI(Graphics User Interface)	도형방식사용자대면부
CUI(Command-line User Interface)	지령행방식사용자대면부
완전가상화	수정되지 않은 가상조작체계를 설치하는 가상화방식으로서 VT 기술을 갖춘 CPU 를 요구합니다.
준가상화	수정된 가상조작체계를 설치하는 가상화방식
대화식가상말단기	가상화서고가 지원하는 지령행방식의 가상체계관리도구의 말단기

제2절. 가상화체계의 설치

1. 가상화체계의 설치를 위한 준비작업

1) 주조작체계의 망설정

가상화지원부를 리용하기에 앞서 주조작체계의 망을 설정합니다.

지령행에서 망 IP 주소가 설정되여있는가를 확인합니다.

```
#ifconfig
```

만일 망장치 eth0 에 IP 주소가 설정되지 않았으면 설정해줍니다.

#ifconfig eth0 172.29.88.61 netmask 255.255.255.0

2) http 봉사기의 시작

가상조작체계를 설치하기에 앞서 http 봉사기를 시작합니다.

체계기동시에 http 봉사기가 시작되여있으면 그대로 두고 만일 체계기동시에 http 봉사기가 시작되여있지 않으면 http 봉사기를 시작합니다.

```
#service httpd start
```

3) 설치판 복사

가상조작체계를 설치하기 위해서는 가상조작체계용 설치판을 미리 복사해두어야 합니다. http 봉사기가 봉사하는 기정등록부에 설치판을 복사합니다. 배포판 CD 를 opt 등록부에 탑재하고 설치판을 http 봉사기가 봉사하는 기정뿌리등록부에 복사합니다.

```
#mount /dev/cdrom /opt
#mkdir /var/www/html/pub
#cp -r /opt /var/www/html/pub
```

주의: ISO 화일에 대한 탑재는 봉사기용체계에서 제공하지 않습니다. 따라서 가상화체계의 설치를 위하여 설치매체를 보관하는 경우에는 ISO 화일로 보관할것이 아니라 원본 그대로 하드디스크에 보관해야 합니다.

2. 패키지의 설치

체계를 설치할 때 가상화관련을 선택하고 체계를 설치합니다. 만일 가상화관련을 선택하지 않고 체계를 설치하였으면 다음의 방법으로 수동으로 설치합니다.

지령행에서 다음의 설치지령으로 설치합니다.

```
#rpm -ivh libvirt-client-0.10.2-18.RSS3.i686.rpm
#rpm -ivh libvirt-python-0.10.2-18.RSS3.i686.rpm
#rpm -ivh libvirt-0.10.2-18.RSS3.i686.rpm
#rpm -ivh qemu-img-0.12.1.2-2.335.RSS3.i686.rpm
#rpm -ivh qemu-kvm-0.12.1.2-2.335.RSS3.i686.rpm
#rpm -ivh python-virtinst-0.600.0-15.RSS3.i686.rpm
```

제3절. 가상화환경의 작업절차

1. 기동중의 가상조작체계의 탈퇴 및 재기동

1) 가상조작체계의 끄기

가상조작체계를 정상으로 끄기하기 위하여 다음의 지령을 사용합니다.

#virsh shutdown [가상조작체계이름 또는 식별자 또는 UUID]

또는 가상조작체계조작탁의 지령행에서 다음의 지령을 실행합니다.

#poweroff

2) 가상조작체계의 재기동

가상조작체계를 재기동하기 위하여 가상조작체계조작탁의 지령행에서 다음의 지령을 실행합니다.

#reboot

3) 가상조작체계의 림시중지

가상조작체계를 림시중지하기 위하여 다음의 지령을 사용합니다.

#virsh suspend [가상조작체계이름 또는 식별자 또는 UUID]

이 지령은 가상조작체계를 림시중지시킵니다. 즉 가상체계가 suspend상태에 있을 때 그것은 체계의 RAM을 소비하지만 처리소자의 자원들을 소비하지는 않습니다. 이 동작은 즉시적인 효력을 가지며 가상체계는 resume선택항목으로 재시작될수 있습니다.

4) 림시중지된 가상조작체계를 재시작

림시중지된 가상조작체계를 재시작하기 위하여 다음의 지령을 사용합니다.

#virsh resume [가상조작체계이름 또는 식별자 또는 UUID]

주의 : 가상조작체계를 설치하는 도중에 가상조작체계의 설치가 응답이 없거나 가상조작체계를 조작하는 과정에 가상조작체계가 응답이 없을 때 즉 비정상적인 상태일 때 다음의 지령으로 가상조작체계를 강제끄기합니다.

#virsh destroy [가상조작체계이름 또는 식별자 또는 UUID]

가상조작체계를 강제끄기한 다음에 가상조작체계를 완전삭제하기 위하여 다음의 지령을 사용합니다.

#virsh undefine [가상조작체계이름 또는 식별자 또는 UUID]

2. 가상화환경의 처리절차들

가상화지원부는 가상조작체계의 설치와 가상조작체계의 관리부분으로 나눌수 있습니다.

1) 가상조작체계의 설치

가상조작체계의 설치는 가상화지원부가 제공하는 지령들과 서고들에 준하여 주조작체계우에서 가상조작체계를 설치하는것입니다.

(1) 가상조작체계용 영상화일의 작성

가상조작체계를 설치하기전에 먼저 가상조작체계용 영상화일을 작성하여야 합니다.

가상조작체계용 영상화일을 작성하기 위하여서는 다음의 지령을 사용합니다.

```
#qemu-img create -f raw /var/lib/libvirt/images/test.img 5G
```

이 지령은 /home 등록부에 test.img 라는 이름으로 5G 바이트용량의 가상조작체계용 영상화일을 작성합니다.

가상조작체계용 영상화일은 가상조작체계를 보관하는 보관소적인 역할을 합니다.

(2) QEMU 가상기계감시기에 련결

먼저 가상조작체계를 설치하기전에 가상화서고에 련결할수 있는 가상기계감시기의 종류를 확인합니다.

가상기계감시기의 종류를 확인하기 위하여 다음의 지령을 실행합니다.

```
#virsh version
```

주조작체계에 설치되여있는 가상기계감시기의 종류가 QEMU 로 확인되면 가상조작체계를 설치합니다.

만일 가상기계감시기의 종류가 QEMU 가 아니면 가상기계감시기의 종류를 QEMU 로 설정합니다.

QEMU 가상기계감시기는 KVM 를 리용하여 완전가상화형태의 가상조작체계를 설치하기 위한 가상기계감시기입니다.

QEMU 가상기계감시기에 련결하기 위하여 다음의 지령을 사용합니다.

```
#virsh --connect qemu:///system
```

주의: 만일 이미 QEMU 가상기계감시기에 련결되여있으면 QEMU 가상기계감시기에 련결하지 않아도 됩니다. 《붉은별》 봉사기용체계 3.0 에서는 QEMU 가상기계감시기만을 지원하므로 이 과정은 생략합니다.

(3) 가상조작체계의 설치

① 가상조작체계설치지령의 실행

가상조작체계설치는 virt-install 지령을 사용하여 설치합니다.

```
#virt-install -n test -r 1024 \
  --file /var/lib/libvirt/images/test.img \
  --nographics -x ‘console=ttyS0’\
  -l /var/www/html/pub
  --security type=static,label=”system_u:system_r:qemu_t:s0-s15:c0.c1023”
```

이 지령은 test 라는 이름으로 가상조작체계를 설치합니다. 가상조작체계가 보관되는 영상화일의 경로는 /home/test.img 입니다. 그리고 가상조작체계설치판이 있는 경로는 /var/www/html/pub 등록부입니다. -r 선택항목은 가상조작체계용으로 할당되는 주기억기의 용량입니다. 이 주기억기의 용량은 최소한 1024MB 이여야 합니다. --nographics 선택항목은 가상조작체계를 도형방식으로 설치하지 않고 지령행방식으로 설치하기 위하여 필요한 선택항목입니다. -x 선택항목은 설치시 kernel 에 넘겨주기 위한 인수입니다. –security 선택항목은 체계의 보안준위를 설정하기 위한 인수입니다.

② 가상조작체계설치

가상조작체계설치지령을 실행하면 주조작체계의 설치쏘프트웨어가 기동하면서 가상조작체계를 설치합니다.

가상조작체계설치시 설치쏘프트웨어에서 주의할점은 다음과 같습니다.

- TCP/IP 설정

설치쏘프트웨어의 TCP/IP 설정창에서 IP 설정을 수동으로 하지 말고 기정값 그대로 설정하여야 합니다.

즉 IP4 와 IP6 을 기정값 그대로 두고 〈확인〉단추를 누릅니다.

- 설치방법

설치쏘프트웨어의 설치방법창에 4 가지가 있습니다.

즉 국부 CD/DVD, 하드구동기, NFS 구동기, URL 이 있습니다.

여기서 URL 을 선택하고 〈확인〉단추를 누릅니다.

URL 설정대화창에서 URL 입력칸에 다음과 같이 입력하고 〈확인〉단추를 누릅니다.

http://172.29.88.61/pub

우의 URL 은 주조작체계의 eth0 망기판의 주소가 172.29.88.61 로 설정된 상태이고 설치 CD 의 내용을 기정 http 봉사등록부인 /var/www/html/pub 에 복사했을 때의 URL 입니다.

만일 install.img 를 찾지 못하는 경우 chmod –R 755 /var/www/html/pub 명령을 실행합니다. 그러나 이것은 보안상 취약점을 가져올수 있으므로 설치가 끝난후에 chmod –R 711 /var/www/html/pub 명령을 실행시켜주어야 합니다.

- 패키지선택

설치쏘프트웨어의 패키지선택창에서 보안체계를 선택하지 말아야 합니다.

또한 가상화지원을 반드시 선택하여야 합니다.

이렇게 선택한 후에 〈확인〉단추를 누릅니다.

2) 가상조작체계의 관리

가상조작체계를 관리하기 위하여서는 가상화서고인 libvirt에 정의된 virsh지령을 사용합니다.

virsh지령은 지령행으로 가상조작체계를 관리하기 위한 가상조작체계관리용 도구입니다.

가상조작체계를 관리하기 위한 virsh지령들에 대한 설명은 표 12과 같습니다.

표 12. 가상조작체계관리지령들

지령	설명
help	기본 도움말정보를 출력합니다.
list	모든 가상체계들을 렬거합니다.
dumpxml	가상체계를 위한 XML구성화일을 출력합니다.
create	XML구성화일로부터 가상체계를 창조하고 새로운 가상체계를 시작합니다.
start	비활성가상체계를 시작합니다.
destroy	가상체계를 강제로 완료시킵니다.
define	가상체계를 위한 XML구성화일을 출력합니다.
domid	가상체계의 ID를 현시합니다.
domuuid	가상체계의 UUID를 현시합니다.
dominfo	가상체계정보를 현시합니다.
domname	가상체계이름을 현시합니다.
domstate	가상체계의 상태를 현시합니다.
quit	내부말단기에서 탈퇴합니다.
resume	림시중지된 가상체계를 재시작시킵니다.
shutdown	가상체계를 훌륭하게 완료합니다.
suspend	가상체계를 림시중지시킵니다.
undefine	가상체계와 련관된 모든 화일들을 삭제합니다.
console	가상체계의 조작탁에로 련결합니다.
define	XML구성화일로부터 가상체계를 정의합니다.

표 13. 가상체계와 가상기계관리기를 감시하기 위한 지령들

지령	설명

connect	인수로 지정한 가상기계감시기에 련결합니다.
version	Virsh 의 판본을 현시합니다.
list	주조작체계우에 설치되여 가상기계감시기에 의해 관리되는 가상체계목록을 현시합니다.
nodeinfo	가상기계감시기에 대한 정보를 출력합니다.

가상조작체계를 화일로 보관하기 위하여 dumpxml 지령을 사용합니다.
이 지령은 가상조작체계를 화일로 보관하였다가 후에 기동하려고 할 때에 유용한 지령입니다.
dumpxml 지령은 다음과 같이 사용합니다.
#virsh dumpxml test > test.xml
또는
#virsh dumpxml test
일단 가상체계를 XML 화일로 보관하면 XML 화일로부터 가상체계를 창조할 수 있습니다. 이때 test 라는 가상체계는 undefine 지령에 의해 이미 삭제되여있어야 합니다.
#virsh create test.xml
이렇게 하면 가상체계가 창조는 되였지만 가상체계가 보이지 않습니다. 그것은 가상체계가 시작되지 않았고 또한 가상체계의 조작탁에 련결되지 않았기때문입니다.
가상체계가 창조되면 start 지령으로 가상체계를 시작합니다.
#virsh start test
가상체계가 시작되여도 가상체계는 보이지 않습니다. 시작된 가상체계를 보기 위하여 console 지령을 사용하여 가상체계의 조작탁에 련결합니다.
#virsh console test
가상체계를 림시중지하기 위하여 suspend 지령을 사용합니다.
이 지령은 체계를 Hibernate 한것과 같은 효과를 나타냅니다.
#virsh suspend test
지령의 실행결과 가상조작체계에 대하여 아무 조작도 할수 없습니다.
가상체계에 대하여 다시 조작하기 위해서는 resume 지령을 사용합니다.
이 지령은 림시중지된 가상체계를 다시 기동시킵니다.
#virsh resume test
기동중의 가상체계를 완료시키기 위하여 shutdown 지령 또는 destroy 지령을 사용합니다.
#virsh shutdown test
또는
#virsh destroy test

여기서 destroy 지령은 가상체계의 응답이 없을 때 즉 가상체계가 폭주상태에 있을 때 가상체계를 강제완료시킵니다.
가상체계를 삭제하기 위하여서는 undefine 지령을 사용합니다.
#virsh undefined test
이 지령은 가상체계가 상태가 활성이 아닐 때 유용합니다.
즉 기동중의 가상체계에 대하여서는 이 지령을 사용할수 없습니다.

3. 가상조작체계정보 사용방법

1) 도움말 보기

가상조작체계용 영상화일작성에 관한 도움말을 보기 위하여 다음의 지령을 실행시킵니다.
#qemu-img --help
#man qemu-img
가상조작체계의 설치에 관한 도움말을 보기 위하여 다음의 지령을 실행시킵니다.
#virt-install --help
#man virt-install
가상조작체계의 관리에 관한 도움말을 보기 위하여 다음의 지령을 실행시킵니다.
#virsh --help
#man virsh

2) 가상조작체계정보보기지령들의 사용

virsh list 지령을 실행했을 때의 출력은 다음과 같습니다.

```
    #virsh list --all
 Id Name State
    ----------------------------------
     0 Domain-0 running
     1 Domain202 paused
     2 Domain010 inactive
     3 Domain9600 crashed
```

virsh net-list 지령을 실행했을 때의 출력은 다음과 같습니다.

```
#virsh net-list --all
Name                    State          Autostart
-----------------------------------
default                 active   yes
```

virsh net-dumpxml 지령을 실행했을 때의 출력은 다음과 같습니다.

```
# virsh net-dumpxml vnet1
<network>
 <name>vnet1</name>
 <uuid>98361b46-1581-acb7-1643-85a412626e70</uuid>
 <forward dev='eth0'/>
 <bridge name='vnet0' stp='on' forwardDelay='0' />
 <ip address='192.168.100.1' netmask='255.255.255.0'>
 <dhcp>
 <range start='192.168.100.128' end='192.168.100.254' />
 </dhcp>
 </ip>
</network>
```

virsh vcpuinfo 지령을 실행했을 때의 출력은 다음과 같습니다.

```
# virsh vcpuinfo r5b2-mySQL01
VCPU: 0
CPU: 0
State: blocked
CPU time: 0.0s
CPU Affinity: yy
```

virsh dumpxml 지령을 실행했을 때의 출력은 다음과 같습니다.

```
#virsh dumpxml r5b2-mySQL01
<domain type='xen' id='13'>
 <name>r5b2-mySQL01</name>
 <uuid>4a4c59a7ee3fc78196e4288f2862f011</uuid>
 <bootloader>/usr/bin/pygrub</bootloader>
 <os>
 <type>linux</type>
 <kernel>/var/lib/libvirt/vmlinuz.2dgnU_</kernel>
 <initrd>/var/lib/libvirt/initrd.UQafMw</initrd>
 <cmdline>ro root=/dev/VolGroup00/LogVol00 rhgb quiet</cmdline>
 </os>
 <memory>512000</memory>
 <vcpu>1</vcpu>
 <on_poweroff>destroy</on_poweroff>
 <on_reboot>restart</on_reboot>
 <on_crash>restart</on_crash>
 <devices>
 <interface type='bridge'>
 <source bridge='xenbr0'/>
```

```
<mac address='00:16:3e:49:1d:11'/>
<script path='vif-bridge'/>
</interface>
<graphics type='vnc' port='5900'/>
<console tty='/dev/pts/4'/>
</devices>
</domain>
```

#virsh dominfo 지령을 실행했을 때의 출력은 다음과 같습니다.

```
#virsh dominfo r5b2-mySQL01
id:                          13
name:     r5b2-mysql01
uuid:     4a4c59a7-ee3f-c781-96e4-288f2862f011
os type:  linux
state:    blocked
cpu(s):   1
cpu time:        11.0s
max memory: 512000kb
used memory:    512000kb
```

4. 자료예비보관

가상조작체계를 설치한 다음에 또는 가상조작체계를 전용화한 다음에 가상조작체계의 예비복사를 만들기 위하여 가상조작체계를 이동합니다.

가상조작체계의 이동은 virsh migrate 지령을 사용하여 진행합니다.

#virsh migrate [--live]

5. 우발사고시 조작과 여러 조작상태들과 방식들

- 가상조작체계설치시 응답이 없거나 가상조작체계자체가 응답이 없을 때 지령행에서 virsh 라고 입력하고 virsh 입력상태로 들어갑니다.

다음의 지령들을 차례로 실행합니다.

#virsh shutdown 가상체계이름

#virsh destroy 가상체계이름

#virsh undefine 가상체계이름

— 조작탁의 쉘환경에서 다음의 지령들을 리용하여 도움말을 볼수 있습니다.

```
#man virsh
#man libvirt
#man virt-install
#virsh --help
#virt-install --help
#man qemu-img
```

제8장. 봉사기감시도구

제1절. 봉사기감시도구의 설치

봉사기감시도구(rssmon)을 리용하려면 rssmon-0.1-1.RSS3.i386.rpm 패키지를 설치하여야 합니다.
먼저 이 패키지가 현체계에 설치되여 있는가를 확인해 봅니다.
지령행에 다음과 같은

#rpm –qa | grep rssmon

지령을 주었을때
rssmon-0.1-1.RSS3.i386.rpm 가 나오지 않으면 이 패키지가 설치되지 않은것이므로 설치를 진행합니다.

설치는 다음과 같이 합니다.

#rpm –ivh rssmon-0.1-1.RSS3.i386.rpm

봉사기감시도구가 정확히 동작하려면 perl 패키지가 설치되여 있어야 합니다. 설치가 끝나면 봉사기감시도구의 설정을 진행합니다.

#rssmon-setup

이때 다음과 같이 초기관리자설정을 진행해야 합니다.

관리자의 식별자:
관리자암호:
암호확인:
포구지정:

여기서 관리자의 식별자와 암호, 포구를 입력하여 등록하면 대몬이 기동합니다.
이때 등록된 식별자와 암호, 포구로 봉사기감시도구에 가입합니다. 일단 관리자의 식별자, 암호, 사용포구가 등록된 후에는 대몬을 기동, 중지, 재기동할 때 문의하지 않습니다.

사용포구를 변경하려는 경우에는 /etc/rssmon/rssmon.conf 화일을 열고
port = 9999
부분에 포구번호를 설정하면 됩니다. 또한 ssl 통신을 리용하지 않으려는 경우에는 이 설정화일에서

ssl = 0
으로 지정하면 됩니다.

제2절. 봉사기감시도구에로의 접속

봉사기감시도구에 접속하려면 원격콤퓨터에서 웨브열람기의 주소란에 다음과 같이 주소를 입력하고 호출합니다.

https://[봉사기 IP 주소]:[포구]

봉사기의 봉사기감시도구가 실행중에 있으면 다음과 같은 가입페지가 펼쳐지게 됩니다.

봉사기감시도구에 가입

172.29.88.62의 봉사기감시도구에 가입할 사용자이름과 암호를 입력해야 합니다.

사용자이름

암호

가입 초기화

가입을 영구적으로 기억하겠습니까?

그림 51. 봉사기감시도구가입페지

여기서 **사용자이름**란에 가입자의 식별자를 입력하고 **암호**란에는 가입자의 암호를 입력합니다.
가입이 성공하면 봉사기감시도구기본페지에 접속하게 됩니다.

그림 52. 봉사기감시도구 기본페지

제3절. 감시도구설정

봉사기감시도구에 대한 설정을 진행하려면 봉사기감시도구의 기본페지에서 **설정**항목을 누릅니다.

여기서는 사용자관리와 감시기록에 대한 설정을 진행할수 있습니다.

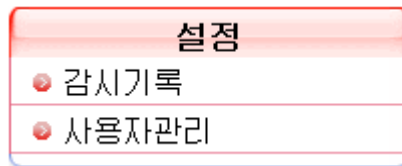



그림 53. 설정항목

1. 사용자관리

사용자관리권한을 가진 사용자만이 이 설정을 진행할수 있습니다.

설정항목의 **사용자관리** 단추를 누르면 사용자관리페지가 펼쳐집니다.

사용자관리

모두 선택 | 선택반전 | 새로운 사용자작성

사용자목록

☐ os ☐ mng

모두 선택 | 선택반전 | 새로운 사용자작성

[선택된 사용자삭제]

그림 54. 사용자관리페지

- 사용자들을 삭제하려면 원하는 사용자들을 선택하고 **선택된 사용자삭제** 단추를 눌러 사용자들을 삭제할수 있습니다.
- 새로운 사용자를 등록하려면 **새로운 사용자작성**항목을 눌러 **사용자정보**페지로 들어갑니다.

사용자정보

사용자정보

사용자이름	
암호	설정 ..
실제이름	

가능한 감시항목들

모두선택 | 선택반전

설정

☐ 감시기록 ☐ 사용자관리

체계상태감시

☐ 열려진 포구목록 ☐ 완전성검사

☐ 통합기록열람기

봉사기상태감시

☐ 웨브봉사기 접근 ☐ 화일봉사기(FTP)

모두선택 | 선택반전

[작성]

그림 55. 사용자정보화면

여기서 사용자이름과 암호, 실제이름을 등록하고 그 사용자의 봉사기감시도구관리권한을 할당하여 줍니다.
다음 **작성** 단추를 눌러 보관합니다.

- 이미 등록된 사용자에 대한 정보를 변경하려면 사용자관리페지에서 사용자의 식별자를 마우스로 선택하여 사용자편집페지로 들어 갑니다.

사용자편집

사용자정보

사용자이름 mng
암호 변경안함
실제이름 채광룡

가능한 감시항목들

모두선택 | 선택반전

설정
감시기록 사용자관리

체계상태감시
열려진 포구목록 완전성검사
통합기록열람기

봉사기상태감시
웨브봉사기 접근 화일봉사기(FTP)
모두선택 | 선택반전

보관

그림 56. 사용자편집

여기서 사용자정보를 수정하고 보관단추를 눌러 수정된 정보를 보관합니다.

2. 감시기록설정

감시기록에 대한 설정을 진행한다. **설정**항목(그림 50)에서 **감시기록** 단추를 눌러 감시기록페지로 들어갑니다.

봉사기감시도구의 리용정형 검색

- 모든 사용자
- 사용자지정 mng
- 이 사용자를 제외하고 mng

- 모든 감시항목
- 이 감시항목에 대하여 CPU리용률감시

- 전체 시간
- 오늘
- 어제
- 년 1 월 일 부터 년 1 월 일 까지

검색

그림 57. 감시기록

이 감시기록화면에서 해당한 항목들을 선택하여 그에 해당한 봉사기감시도구의 리용정형을 열람할수 있습니다.

봉사기감시도구를 리용한 사용자와 감시항목, 리용시간을 선택하고 **검색**단추를 눌러 결과를 봅니다.

검색결과

사용자 os의 감시기록 (2013/1/01 부터 2013/5/27까지

날자	시간	감시항목	동작	사용자	의뢰기주소
2013/5/27	19:31	완전성검사	열람	os	172.29.88.65
2013/5/27	19:31	열려진 포구목록	열람	os	172.29.88.65
2013/5/27	19:28	완전성검사	열람	os	172.29.88.65
2013/5/27	19:27	완전성검사	열람	os	172.29.88.65
2013/5/27	19:27	완전성검사	열람	os	172.29.88.65
2013/5/27	19:27	완전성검사	열람	os	172.29.88.55
2013/5/27	19:27	열려진 포구목록	열람	os	172.29.88.55
2013/5/27	19:27	완전성검사	열람	os	172.29.88.65
2013/5/27	19:26	완전성검사	열람	os	172.29.88.65
2013/5/27	19:26	열려진 포구목록	열람	os	172.29.88.65
2013/5/27	19:19	열려진 포구목록	열람	os	172.29.88.65

그림 58. 봉사기감시도구리용정형검색결과

선택한 사용자들과 리용항목, 시간에 해당한 검색결과를 항목별로 자세히 보여줍니다.

제4절. 체계상태감시

체계상태에 대한 감시를 진행하려면 봉사기감시도구의 기본페지에서 **체계상태감시**항목을 누릅니다.

그러면 다음과 같은 체계상태감시항목이 펼쳐집니다.

체계상태감시
CPU리용률감시
기억기리용률감시
망통화량감시
열려진 포구목록
완전성검사
통합기록열람기

그림 59. 체계상태감시

목록에 제시된 항목을 선택함으로써 해당상태에 대한 감시를 진행할수 있다.

1. CPU 리용률감시

체계상태감시목록(그림 53)에서 **CPU 리용률감시**단추를 누릅니다.

이때 펼쳐지는 **CPU 리용률감시**창문에서 CPU 리용정형에 대한 정보를 그라프로 현시해줍니다.

2. 기억기리용률감시

체계상태감시목록(그림 53)에서 **기억기리용률감시**단추를 누릅니다.

이때 펼쳐지는 **기억기리용률감시**창문에서 기억기리용에 대한 정보를 그라프로 현시해줍니다.

3. 망통화량감시

체계상태감시목록(그림 53)에서 **망통화량감시**단추를 누릅니다.
이때 펼쳐지는 **망통화량감시**창문에서 망통화상태를 감시합니다.

4. 열려진 포구목록

열려진 포구에 대한 감시를 진행합니다.
체계상태감시목록에서 열려진 **포구목록**단추를 누릅니다.
그러면 다음과 같은 열려진 포구목록페지가 펼쳐집니다.

열려진 포구목록

포구번호	규약	봉사이름
22	tcp	ssh
25	tcp	smtp
80	tcp	http
111	tcp	rpcbind
443	tcp	https
631	tcp	ipp
15000	tcp	hydap
16000	tcp	fmsas

그림 60.열려진 포구목록

현재 열려진 포구들에 대하여 포구번호와 그 포구로 통신하는 전송규약, 그리고 현재진행중인 봉사이름을 보여줍니다.

5. 완전성검사

체계상태감시목록에서 열려진 **완전성검사**단추를 누릅니다.
이때 완전성검사페지가 펼쳐지는데 날자와 시간, 원천, 내용이 페지별로 현시됩니다.

완전성검사

처음이전 1/2 다음마지막

날자	시간	원천	내용
2013-05-26	06:27:58	"/bin/traceroute"	"접근권한, 색인마디, 고정련결수, 사용자ID, 집단ID, 크기, 블로크수, 수정시간, 생성시간, MD5, SHA1, SHA256, 이동, 삭제";
2013-05-26	17:31:12	/bin/traceroute	화일이 존재하지 않습니다.;
2013-05-27	16:16:55	/bin/traceroute	화일이 존재하지 않습니다.;
2013-05-27	16:32:28	/bin/traceroute	화일이 존재하지 않습니다.;
2013-05-27	16:35:02	/bin/traceroute	화일이 존재하지 않습니다.;
2013-05-27	19:53:11	/bin/traceroute	화일이 존재하지 않습니다.;
2013-05-27	20:03:25	/bin/traceroute	화일이 존재하지 않습니다.;
2013-05-27	20:42:36	/bin/traceroute	화일이 존재하지 않습니다.;
2013-05-27	21:01:47	/bin/traceroute	화일이 존재하지 않습니다.;
2013-05-27	21:05:00	/bin/traceroute	화일이 존재하지 않습니다.;

그림 61. 완전성검사

6. 통합기록열람기

체계상태감시목록에서 열려진 **통합기록열람기**단추를 누릅니다.
자세한 내용은 “KUTOS11-프로 1.0-18 사용 1.0-봉사기 3.0-02.doc”의 제 3 장 제 12 절을 참고하십시오.

제5절. 봉사기상태감시

봉사기상태에 대한 감시를 진행하려면 봉사기감시도구의 기본페지에서 **봉사기상태감시**항목을 누릅니다.
그러면 다음과 같은 봉사기상태감시항목이 펼쳐집니다.

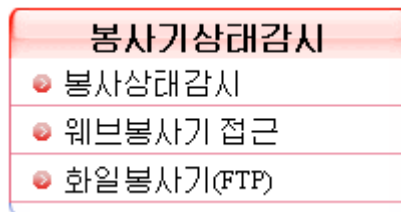



그림 62. 봉사기상태감시

목록에 제시된 항목을 선택함으로써 해당상태에 대한 감시를 진행할수 있다.

1. 웨브봉사기접근

봉사기상태감시목록(그림 56)의 **웨브봉사기접근**항목을 선택합니다.

이때 펼쳐지는 웨브봉사기접근페지에서 웨브봉사기접근에 관한 자세한 정보목록을 볼수 있습니다.

2. 화일봉사기(FTP)

봉사기상태감시목록(그림 56)의 **화일봉사기(FTP)**항목을 선택합니다.

이때 펼쳐지는 화일봉사기(FTP)화면에서 웨브봉사기접근에 관한 자세한 정보목록을 볼수 있습니다.

색 인